bitdefender
total security 2010

Manuale dell'utente

Diritto d'autore© 2010 BitDefender

Sicurezza totale BitDefender 2010
Manuale dell'utente

Pubblicato 2010.04.19

Diritto d'autore© 2010 BitDefender

Avvertimenti Legali

Tutti i diritti riservati. Nessuna parte di questo manuale può essere riprodotta o trasmessa in alcuna forma o tramite qualsiasi strumento, elettronico o meccanico, incluse fotocopie, registrazioni, o attraverso qualsiasi informazione di archivio o sistema di recupero dati, senza un permesso scritto di BitDefender, ad eccezione di brevi citazioni nelle rassegne menzionando la provenienza. Il contenuto non può essere modificato in nessun modo.

Avvertenze e Limiti. Questo prodotto e la sua doumentazione sono protetti dal Copyright. L'informazione su questo documento è fornita sul concetto «così com'è» senza garanzia. Sebbene ogni precauzione è stata adottata nella preparazione di questo documento, gli autori non hanno alcun obbligo nei confronti di alcuna persona o entità rispetto ad alcuna perdita o danneggiamento causati o che si presume essere stati causati, direttamente o indirettamente, dalle informazioni contenute in questo lavoro.

Questo manuale contiene collegamenti a siti Internet terze parti, che non sono sotto il controllo della BitDefender, conseguentemente la BitDefender non è responsabile per il contenuto di qualsiasi sito collegato. Se accedi a siti Internet di terze parti, menzionate in questo manuale, lo farai assumendotene tutti i rischi. BitDefender fornisce tali collegamenti solo come una convenienza, e l'inclusione dei collegamenti non implica che BitDefender approva o accetta alcuna responsabilità per il contenuto di questi siti di terze parti.

Marchi Registrati. Nomi e marchi registrati possono essere citati in questo libro. Tutti I marchi registrati e non in questo documento sono di sola proprietà dei loro rispettivi proprietary.

bitdefender

Indice

Accettamento della Licenza per utenti finali xii

Prefazione xviii
1. Convenzioni usate in questo manuale xviii
1.1. Convenzioni tipografiche xviii
1.2. Avvertenze xviii
2. Struttura del manuale xix
3. Richiesta di commenti xx

Installazione e rimozione 1

1. Requisiti del sistema 2
1.1. Requisiti minimi di sistema 2
1.2. Requisiti di sistema consigliati 2
1.3. Software supportato 2

2. Preparazione all'Installazione 4

3. Installazione di BitDefender 5
3.1. Procedura guidata di Registrazione 8
3.1.1. Passo 1 - Registrare BitDefender Total Security 2010 9
3.1.2. Passo 2 - Creare un Account BitDefender 10
3.2. Procedura guidata di Configurazione 12
3.2.1. Passo 1 - Selezione del Profilo di Utilizzo 12
3.2.2. Passo 2 - Descrivere il Computer 13
3.2.3. Passo 3 - Selezionare l'Interfaccia Utente 14
3.2.4. Passo 4 - Configurazione Controllo Genitori 15
3.2.5. Passo 5 - Configurazione Rete BitDefender 16
3.2.6. Passo 6 - Selezionare le Attività da eseguire 17
3.2.7. Passo 7 - Fine 18

4. Upgrade 20

5. Riparare o Rimuovere BitDefender 21

Iniziando 22

6. Panoramica 23
6.1. Apertura di BitDefender in corso 23
6.2. Modalità di visualizzazione dell'interfaccia dell'utente. 23
6.2.1. Modalità inesperto 24
6.2.2. Modalità intermedia 27
6.2.3. Modalità avanzata 29
6.3. Icona barra delle applicazioni 32
6.4. Barra di Attività della Scansione 33
6.4.1. Scansiona File e Cartelle 33
6.4.2. Disabilita/ripristina la barra di attività scansione 34
6.5. Scansione Manuale di BitDefender 34
6.6. Modalità giochi e Modalità portatile 36

6.6.1. Modalità giochi 36
6.6.2. Modalità Portatile 38
6.7. Rilevamento dispositivo automatico 38

7. Risolvi i Problemi 40
7.1. Assistente Risolti Tutti i Problemi 40
7.2. Configurazione del monitoraggio problemi 42

8. Configurazione delle Impostazioni fondamentali 44
8.1. Impostazioni interfaccia utente 45
8.2. Impostazioni di sicurezza 46
8.3. Impostazioni generali 48

9. Cronologia ed Eventi 50

10. Registrazione e Il mio Account 52
10.1. Registrazione Sicurezza totale BitDefender 2010 52
10.2. Attivazione di BitDefender 53
10.3. Acquisto di chiavi di licenza 56
10.4. Rinnovo della Licenza 56

11. Procedure guidate 57
11.1. Procedura guidata scansione antivirus 57
11.1.1. Passo 1/3 – Scansione 57
11.1.2. Passo 2/3 – Selezionare Azioni 59
11.1.3. Passo 3/3 – Visualizzare risultati 60
11.2. Assistente Scansione Personalizzata 62
11.2.1. Passo 1/6 - Finestra di Benvenuto 62
11.2.2. Passo 2/6 - Selezionare Target 63
11.2.3. Passo 3/6 - Selezionare Azioni 64
11.2.4. Passo 4/6 - Impostazioni Aggiuntive 66
11.2.5. Passo 5/6 - Scansione 67
11.2.6. Passo 6/6 – Visualizzare Risultati 68
11.3. Procedura guidata di Controllo delle vulnerabilità 69
11.3.1. Passo 1/6 – Selezionare le Vulnerabilità da controllare. 70
11.3.2. Passo 2/6 - Controllare Vulnerabilità 71
11.3.3. Passo 3/6 - Aggiornare Windows 72
11.3.4. Passo 4/6 - Aggiornare le Applicazioni 73
11.3.5. Passo 5/6 - Cambiare password deboli 74
11.3.6. Passo 6/6 – Visualizzare Risultati 75
11.4. Assistenti di Backup e di Ripristino 75
11.4.1. Assistente Backup Locale 76
11.4.2. Assistente Recupero Locale 81
11.5. Assistenti di Ottimizzazione 84
11.5.1. Procedura guidata Deframmentazione Disco 84
11.5.2. Procedura guidata pulizia PC 88
11.5.3. Procedura guidata Ricercatore di Duplicati 91
11.5.4. Procedura guidata Pulitore Registro 95
11.5.5. Procedura guidata Ripristino Registro 100
11.5.6. Procedura guidata distruzione file 102
11.6. Assistente File Vault 105

11.6.1. Aggiungi file alla Criptazione (Vault) ... 106
11.6.2. Rimuovi Vault File ... 111
11.6.3. Visualizza File Vault ... 116
11.6.4. Blocca File Vault ... 120

Modalità intermedia ... 124

12. Dashboard ... 125

13. Sicurezza ... 127
13.1. Area di Stato ... 127
13.1.1. Configurazione del Monitoraggio Stato ... 128
13.2. Funzioni Veloci ... 130
13.2.1. Aggiornamento di BitDefender ... 130
13.2.2. Scansione con BitDefender ... 131
13.2.3. Ricerca delle Vulnerabilità ... 132
13.2.4. Configurazione Controllo Genitori ... 133

14. Tune-Up ... 134
14.1. Area di Stato ... 134
14.1.1. Configurazione del Monitoraggio Stato ... 135
14.2. Funzioni Veloci ... 135
14.2.1. Pulizia del Registro di Windows ... 136
14.2.2. Recupero di Registro Cancellato ... 136
14.2.3. Trovare file duplicati ... 137
14.2.4. Pulizia del vostro PC ... 137
14.2.5. Eliminazione Definitiva dei File ... 138
14.2.6. Deframmentazione dei Volumi del Disco Rigido. ... 138

15. Archiviazione File ... 140
15.1. Area di Stato ... 141
15.2. Funzioni Veloci ... 142

16. Rete ... 143
16.1. Funzioni Veloci ... 143
16.1.1. Unirsi alla Rete BitDefender ... 144
16.1.2. Aggiungere dei computer alla Rete BitDefender ... 144
16.1.3. Gestione della Rete BitDefender ... 146
16.1.4. Scansione di tutti i computer ... 149
16.1.5. Aggiornamento di tutti i Computer ... 149
16.1.6. Registrazione di Tutti i Computer ... 150

Modalità avanzata ... 151

17. Generale ... 152
17.1. Dashboard ... 152
17.1.1. Stato generale ... 153
17.1.2. Statistiche ... 156
17.1.3. Panoramica ... 156
17.2. Impostazioni ... 157
17.2.1. Impostazioni generali ... 158

17.2.2. Impostazioni del Report sui virus ... 160
17.3. Sistema Informazione ... 160

18. Antivirus ... 162
18.1. Protezione in tempo reale ... 162
18.1.1. Configurazione del Livello di Protezione ... 163
18.1.2. Livello di Protezione Personalizzato ... 164
18.1.3. Configurazione Active Virus Control ... 168
18.1.4. Disattivazione Protezione in Tempo Reale ... 171
18.1.5. Configurazione della Protezione Antiphishing ... 171
18.2. Scansione a richiesta ... 172
18.2.1. Impostazioni della Scansione ... 174
18.2.2. Utilizzo del Menu Rapido ... 175
18.2.3. Creazione delle Funzioni di Scansione ... 176
18.2.4. Configurare un Compito di Scansione ... 176
18.2.5. Scansione file e cartelle ... 187
18.2.6. Visualizzazione dei Registri di Scansione ... 196
18.3. Oggetti esclusi dalla scansione ... 197
18.3.1. Esclusione dei Percorsi dalla Scansione ... 199
18.3.2. Esclusione delle Estensioni dalla Scansione ... 202
18.4. Area di Quarantena ... 206
18.4.1. Gestione dei File in Quarantena ... 207
18.4.2. Configurazione delle Impostazioni di Quarantena ... 208

19. Antispam ... 210
19.1. Approfondimenti Antispam ... 210
19.1.1. Filtri Antispam ... 210
19.1.2. Operazione Antispam ... 212
19.1.3. Aggiornamenti Antispam ... 213
19.2. Stato ... 213
19.2.1. Impostazione del Livello di Protezione ... 214
19.2.2. Configurazione dell'Elenco Amici ... 215
19.2.3. Configurazione dell'Elenco Spammer ... 217
19.3. Impostazioni ... 219
19.3.1. Impostazioni Antispam ... 220
19.3.2. Filtri Antispam ... 221
19.3.3. Filtri Avanzati Antispam ... 221

20. Controllo genitori ... 222
20.1. Configurazione del Controllo Genitori per un utente ... 223
20.1.1. Protezione delle Impostazioni del Controllo dei Genitori ... 225
20.1.2. Impostazione della Categoria di Età ... 226
20.2. Controllo Attività dei Bambini ... 229
20.2.1. Controllo dei Siti Web visitati ... 230
20.2.2. Configurazione Notifiche E-mail ... 230
20.3. Controllo Web ... 231
20.3.1. Creazione Regole di Controllo Web ... 232
20.3.2. Gestione delle Regole di Controllo Web ... 233
20.4. Limitatore di Tempo su Web ... 234
20.5. Controllo applicazioni ... 235
20.5.1. Creazione Regole di Controllo Applicazioni ... 235

20.5.2. Gestione Regole di Controllo Applicazioni ... 237
20.6. Controllo parole chiave ... 237
20.6.1. Creazione Regole di Controllo Parole Chiave ... 238
20.6.2. Gestione delle Regole di Controllo Parole Chiave ... 239
20.7. Controllo del Chat (IM) ... 240
20.7.1. Creazione di regole di controllo della messaggistica istantanea (IM) ... 241
20.7.2. Gestione di regole di controllo della messaggistica istantanea (IM) ... 241

21. Controllo della Privacy ... 243
21.1. Statistiche Controllo Privacy ... 243
21.1.1. Configurazione del Livello di Protezione ... 244
21.2. Controllo Identità ... 244
21.2.1. Creazione delle Regole d'Identità ... 247
21.2.2. Definizione Esclusioni ... 250
21.2.3. Amministrazione delle regole ... 251
21.2.4. Regole definite da altri amministratori ... 252
21.3. Controllo dei Registri ... 252
21.4. Controllo dei Cookie ... 254
21.4.1. Finestra di Configurazione ... 256
21.5. Controllo script ... 258
21.5.1. Finestra di Configurazione ... 259

22. Firewall ... 261
22.1. Impostazioni ... 261
22.1.1. Impostare l'Azione di Default ... 262
22.1.2. Configurazione delle Impostazioni Avanzate del Firewall ... 263
22.2. Rete ... 265
22.2.1. Modifica del Livello di Fiducia ... 266
22.2.2. Configurare la Modalità Invisibile ... 267
22.2.3. Configurare le Impostazioni Generali ... 267
22.2.4. Zone di rete ... 267
22.3. Regole ... 268
22.3.1. Aggiungere Regole Automaticamente ... 270
22.3.2. Eliminazione e ripristino delle regole ... 271
22.3.3. Creare e modificare delle Regole ... 271
22.3.4. Gestione Avanzata delle Regole ... 275
22.4. Controllo Connessione ... 277

23. Vulnerabilità ... 279
23.1. Stato ... 279
23.1.1. Correggi Vulnerabilità ... 280
23.2. Impostazioni ... 280

24. Backup ... 282
24.1. Impostazioni del Backup ... 283
24.1.1. Inizia ... 284
24.1.2. Gestione processo ... 285
24.1.3. Registro ... 303
24.1.4. Toolbox ... 306
24.1.5. Barra di Menu ... 308

25. Criptazione 311
25.1. Criptazione Chat (IM) 311
25.1.1. Disabilitare la Criptazione per Utenti Specifici 312
25.2. Criptazione file 313
25.2.1. Creare un Vault 314
25.2.2. Aprire un Vault 316
25.2.3. Bloccare un Vault 316
25.2.4. Cambiare la Password del Vault 317
25.2.5. Aggiungere dei File ad un Vault 318
25.2.6. Rimuovere dei File da un Vault 318
26. Tune-Up 320
26.1. Deframmentazione dei Volumi del Disco Rigido. 321
26.2. Pulizia del vostro PC 321
26.3. Eliminazione Definitiva dei File 322
26.4. Pulizia del Registro di Windows 323
26.5. Recupero di Registro Cancellato 323
26.6. Trovare file duplicati 324
27. Modalità Gioco / Portatile 325
27.1. Modalità giochi 325
27.1.1. Configurazione Automatica della Modalità Gioco 326
27.1.2. Gestione della Lista dei Giochi 327
27.1.3. Configurazione delle Impostazioni della Modalità Gioco 328
27.1.4. Modifica Hotkey della Modalità Gioco. 329
27.2. Modalità Portatile 330
27.2.1. Configurazione delle Impostazioni della Modalità Portatile 331
28. Rete domestica 333
28.1. Unirsi alla Rete BitDefender 333
28.2. Aggiungere dei computer alla Rete BitDefender 334
28.3. Gestione della Rete BitDefender 336
29. Aggiorna 339
29.1. Aggiornamento Automatico 339
29.1.1. Richiedere un aggiornamento 340
29.1.2. Disattivare Aggiornamento Automatico 341
29.2. Impostazioni dell'aggiornamento 341
29.2.1. Impostare Ubicazioni Aggiornamento 342
29.2.2. Configurazione Aggiornamento Automatico 343
29.2.3. Configurazione Aggiornamento Manuale 343
29.2.4. Configurazione delle Impostazioni Avanzate 343
29.2.5. Gestione Proxies 344
30. Registrazione 347
30.1. Registrazione Sicurezza totale BitDefender 2010 347
30.2. Creazione di un Account BitDefender 348
Integrazione in Software Windows e di terzi 351
31. Integrazione nel Menu Contestuale Windows 352

31.1. Scansiona con BitDefender ... 352
31.2. Criptazione File (File Vault) BitDefender ... 353
31.2.1. Crea Vault ... 354
31.2.2. Apri Vault ... 355
31.2.3. Blocca Vault ... 356
31.2.4. Aggiungi a file vault ... 357
31.2.5. Rimuovi dal file vault ... 357
31.2.6. Cambiare la Password del Vault ... 357
31.3. Distruggi file ... 358
32. Integrazione nei Web Browser ... 360
33. Integrazione in Programmi Instant Messenger ... 363
34. Integrazione nei client di posta ... 364
34.1. Assistente per la Configurazione Antispam ... 364
34.1.1. Passo 1/6 - Finestra di Benvenuto ... 365
34.1.2. Passo 2/6 - Compilare l' Elenco Amici ... 366
34.1.3. Passo 3/6 - Cancellare il Database Bayesiano ... 367
34.1.4. Passo 4/6 - Istruzione del Filtro Bayesiano con messaggi e-mail Leciti ... 368
34.1.5. Passo 5/6 - Istruzione del Filtro Bayesiano con SPAM ... 369
34.1.6. Passo 6/6 – Sommario ... 370
34.2. Barra degli Strumenti Antispam ... 370
Come fare ... 379
35. Scansione di file e cartelle ... 380
35.1. Utilizzando il Menu Contestuale Windows ... 380
35.2. Utilizzando attività di scansione ... 380
35.3. Utilizzo della Scansione Manuale di BitDefender ... 382
35.4. Utilizzo della Barra delle Attività di Scansione ... 384
36. Programmazione della scansione del computer ... 385
37. Come effettuare il backup dei dati ... 387
38. Come ripristinare i dati di backup ... 389
Risoluzione dei problemi e aiuto ... 390
39. Risoluzione dei problemi ... 391
39.1. Problemi di installazione ... 391
39.1.1. Errori di convalida dell'installazione ... 391
39.1.2. Installazione non riuscita ... 392
39.2. I servizi BitDefender non rispondono ... 394
39.3. La condivisione file e stampanti sulla Rete Wi-Fi (Wireless) non funziona. ... 394
39.3.1. Soluzione "Computer Affidabili" ... 395
39.3.2. Soluzione "Rete Sicura" ... 397
39.4. Il filtro Antispam non funziona appropriatamente ... 398
39.4.1. Messaggi Legittimi sono contrassegnati come [spam] ... 399
39.4.2. Molti Messaggi Spam non vengono rilevati ... 402

39.4.3. Il Filtro Antispam non rileva alcun messaggio spam 404
39.5. Rimozione di BitDefender non riuscita 405
40. Supporto 407
40.1. BitDefender Knowledge Base(Archivio D'informazione BitDefender) 407
40.2. Chiedere Aiuto 407
40.3. Informazioni di Contatto: 408
40.3.1. Indirizzi Web 408
40.3.2. Uffici BitDefender 408
CD di soccorso BitDefender 410
41. Panoramica 411
41.1. Requisiti del sistema 411
41.2. Software Incluso 412
42. BitDefender Rescue CD fai-da-te. 415
42.1. Avviare BitDefender Rescue CD 415
42.2. Arrestare BitDefender Rescue CD 416
42.3. Come eseguo una scansione antivirus? 417
42.4. Come Configurare la connessione Internet? 418
42.5. Come aggiornare BitDefender? 419
42.5.1. Come aggiornare BitDefender attraverso un proxy? 420
42.6. Come posso salvare ai miei dati? 421
42.7. Come si usa la modalità console? 423
Glossario 424

Accettamento della Licenza per utenti finali

SE NON SI ACCETTANO I TERMINI E LE CONDIZIONI NON INSTALLARE IL SOFTWARE. SELEZIONANDO "ACCETTO", "OK", "CONTINUA", "SI", OPPURE INSTALLANDO O UTILIZZANDO IN OGNI CASO IL SOFTWARE, STATE INDICANDO IL VOSTRO COMPLETO BENESTARE E ACCETTANDO I TERMINI DI QUESTO ACCORDO.

REGISTRAZIONE DEL PRODOTTO. Con l'accettazione del presente accordo, l'Utente si impegna a registrare il software, utilizzando il pulsante "Il mio account", come condizione del proprio utilizzo del Software (e ricezione degli aggiornamenti) e il diritto di manutenzione. Questo controllo contribuisce a far sì che il software funzioni solo su computer che hanno una licenza valida e che solo gli utenti finali con Licenza valida possano ricevere servizi di manutenzione. La registrazione richiede un prodotto con un numero di serie valido e un indirizzo e-mail valido per il rinnovo e altri avvisi.

Questi termini ricoprono le Soluzioni e i Servizi BitDefender per gli utilizzatori Home, incluse le documentazioni relative e qualsiasi aggiornamento e rinnovo delle applicazioni rese disponibili dalla licenza acquistata o qualsiasi servizio in accordo a quanto definito nella documentazione e ogni copia di questa.

Questo accordo di Licenza è un contratto legale tra te (utente finale o individuale o entità singola) e BITDEFENDER, per l'utilizzo dei prodotti Software BITDEFENDER identificati sopra, che include il software e può includere supporti digitali, materiale stampato, e documentazione "online" oppure elettronica (qui di seguito designata come "BitDefender"), tutti protetti dalle leggi degli Stati Uniti ed internazionali sul copyright, e trattati di protezione internazionali. Mediante l'installazione, copia, o qualsiasi uso di BitDefender, accetti di essere vincolato ai termini di questo accordo. Se non accetti i termini di questo accordo, non installare ne usare BitDefender; puoi, in ogni caso, riportarlo al tuo punto vendita per il rimborso completo dell'importo versato, entro 30 giorni dall'acquisto del quale potrà essere richiesta una ricevuta.

Se non si è d'accordo con i termini che determinano il contratto di utilizzo della licenza, non installare o utilizzare BitDefender.

Licenza BitDefender. BitDefender è protetto da leggi e trattati internazionali su copyright, così come da altre leggi e trattati sulla proprietà intellettuale. BitDefender è autorizzato, non venduto.

CONCESSIONE DI LICENZA. BITDEFENDER concede,solamente all'utente che l'ha acquistata e non a terzi, la presente licenza non esclusiva, limitata, non assegnabile, non trasferibile, non concedibile in ulteriore licenza e produttrice di royalties, a utilizzare BitDefender.

APPLICAZIONE DEL SOFTWARE. Si può installare e usare BitDefender, su quanti computers è necessario ma limitatamente al numero totale di utenti autorizzati dalla licenza. E' possibile fare una copia addizionale di back-up.

LICENZA UTENTE DESKTOP. Questa licenza si applica al software BitDefender che può essere installato su un computer singolo e che non fornisce servizi di rete. Ogni utente principale può installare questo software su un computer singolo e può eseguire una copia aggiuntiva per il backup su un dispositivo diverso. Il numero di utenti principali consentito è il numero di utenti della licenza.

PERIODO DI LICENZA. Il periodo di validità, avrà inizio dalla data in cui viene eseguita l'installazione, la copia, o quando viene usato in qualche modo, per la prima volta, BitDefender, e continuerà solamente sul computer dove è stato originariamente installato.

SCADENZA. Il prodotto cesserà di compiere le sue funzioni immediatamente dopo la scadenza della licenza.

UPGRADE (AGGIORNAMENTO). Se BitDefender è identificato come un upgrade, per usarlo devi essere stato autorizzato precedentemente ad utilizzare un prodotto classificato da BITDEFENDER come idoneo all' aggiornamento. Un prodotto BitDefender classificato come upgrade, sostituisce o complementa il prodotto originariamente installato e idoneo. Puoi usare il prodotto aggiornato esclusivamente in conformità con i termini di questo Accordo di Licenza. Se BitDefender è l' upgrade di un componente di un pacchetto di programmi software, dato in licenza come un solo prodotto, può essere utilizzato e trasferito solamente come parte integrante di questo pacchetto e non può essere separato per l'utilizzo su più di un computer.

COPYRIGHT. Tutti i diritti, titoli, e interessi derivati da o verso BitDefender e tutti i diritti di copyright derivati da o verso BitDefender (includendo ma non limitando qualsiasi immagine, fotografia, logo, animazione, video, audio, musica, testo e "applets" incorporati nel BitDefender) il materiale stampato allegato e qualsiasi copia di BitDefender sono proprietà della BITDEFENDER. BitDefender è protetto dalle leggi di copyright e da quanto previsto dai trattati internazionali. Di conseguenza, BitDefender deve essere considerato come qualunque altro materiale protetto da copyright ad eccezione del fatto che è possibile installare BitDefender su un singolo computer conservando l'originale esclusivamente per scopi di backup o archiviazione. Non è permessa la copia o riproduzione del materiale stampato e allegato al prodotto o supporto BitDefender. In tutte le copie create indipendentemente dal supporto o formato in cui vi sia BitDefender, è necessario riprodurre ed includere tutte le note copyright in formato originale. Non è permesso noleggiare a terzi, vendere, dare in leasing, la licenza di BitDefender. Non è permesso smontare, raggruppare, disassemblare, creare lavori derivati, modificare, tradurre né fare alcun tentativo per scoprire, individuare, il codice fonte di BitDefender.

GARANZIA LIMITATA. BITDEFENDER garantisce che il supporto con il quale viene distribuito BitDefender è esente da difetti per un periodo di trenta giorni dalla data in cui viene consegnato. In caso di difettosità riscontrate, BITDEFENDER, a sua discrezione, potrà sostituire il supporto, oppure rimborsare l'importo pagato per l'acquisto, a fronte di una ricevuta. BITDEFENDER non garantisce che BitDefender sarà sempre privo di errori o che gli errori verranno comunque corretti. BITDEFENDER

non garantisce che BitDefender soddisferà le necessità dell'utilizzatore. BITDEFENDER CON LA PRESENTE NEGA QUALSIASI ALTRA GARANZIA PER BITDEFENDER, SIA ESPLICITA CHE IMPLICITA. LA SUDDETTA GARANZIA E' ESCLUSIVA E SOSTITUISCE TUTTE LE ALTRE GARANZIE, SIA ESPLICITE CHE IMPLICITE, INCLUDENDO LE GARANZIE DI COMMERCIABILITA', DI ADEGUAMENTO AD UN PROPOSITO PARTICOLARE, O DI NON INFRAZIONE. QUESTA GARANZIA CONCEDE DIRITTI LEGALI SPECIFICI CHE POSSONO VARIARE DA STATO A STATO.

ECCETTO PER QUANTO CHIARAMENTE SOTTOLINEATO IN QUESTO ACCORDO, ESPRESSAMENTE O IMPLICITAMENTE, RISPETTO AI PRODOTTI, AI MIGLIORAMENTI, ALLA MANUTENZIONE O AL SUPPORTO AD ESSI RELATIVI, O A QUALSIASI ALTRO MATERIALE (TANGIBILE O INTANGIBILE) O SERVIZIO FORNITO DA QUESTI. BITDEFENDER QUI DISCONOSCE ESPRESSAMENTE QUALSIASI GARANZIA E CONDIZIONE IMPLICITA, INCLUSO, SENZA LIMITAZIONE, LE GARANZIE IMPLICITE DI COMMERCIABILITÀ, APPROPRIATEZZA PER UNO SCOPO PARTICOLARE, TITOLO, NON INTERFERENZA, ACCURATEZZA DEI DATI, ACCURATEZZA DEL CONTENUTO INFORMATIVO, INTEGRAZIONE DEL SISTEMA, E NON VIOLAZIONE DEI DIRITTI DI TERZE PARTI ATTRAVERSO IL FILTRO, LA DISABILITAZIONE, O LA RIMOZIONE DI TALE SOFTWARE, SPYWARE, ADWARE, COOKIE, E-MAIL, DOCUMENTI, PUBBLICITÀ O SIMILI, DI TERZE PARTI, CHE SI ORIGININO DA STATUTO, LEGGE, CORSO DI TRATTATIVE, COSTUMI E PRATICA, O USI DEL COMMERCIO.

DECLINAZIONE DELLE RESPONSABILITA' DI DANNI. Chiunque utilizzi, provi oppure valuti BitDefender, si assume tutto il rischio della qualità e delle prestazioni di BitDefender. In nessun caso BITDEFENDER sarà ritenuta responsabile di qualunque danno di qualsiasi tipo, inclusi senza limitazioni, danni diretti o indiretti derivati dall' utilizzo, o la consegna di BitDefender, anche nel caso in cui BITDEFENDER sia informata dell'esistenza o la possibilità che tali danni possano verificarsi. ALCUNI STATI NON CONSENTONO LA LIMITAZIONE O L' ESCLUSIONE DI RESPONSABILITA' PER DANNI ACCIDENTALI O CONSEGUENTI, IN QUEL CASO LA LIMITAZIONE O ESCLUSIONE SOPRA INDICATA NON POTRA' ESSERE APPLICATA. IN NESSUN CASO COMUNQUE, LA RESPONSABILITA' DI BITDEFENDER POTRA' ECCEDERE IL PREZZO CHE PAGATO PER L'ACQUISTO DI BITDEFENDER. Le restrizioni e limitazioni fissate saranno applicate indipendentemente dal modo in cui si accetta di usare, valutare o provare BitDefender.

Alcuni stati non consentono la limitazione o l'esclusione di responsabilità per danni incidentali o consequenziali, per cui la succitata limitazione o l'esclusione non può applicarsi a voi.

In nessun caso BitDefender ha la responsabilità di risarcire un prezzo di acquisto più alto pagato da voi per BitDefender. Le rinunce e le limitazioni di cui sopra si applicano indipendentemente dal fatto che si accetta di utilizzare, valutare, o testare BitDefender.

AVVISO IMPORTANTE AGLI UTENTI. AVVISO IMPORTANTE AGLI UTENTI. QUESTO SOFTWARE NON E ESENTE DA EVENTUALI DIFETTI PROVOCATI ANCHE DALL'UTILIZZO

DELLO STESSO, E NON E' STATO PROGETTATO NE' DESTINATO ALL'USO IN AMBIENTI PERICOLOSI CHE RICHIEDANO OPERAZIONI O ATTIVITA' IN MANCANZA DI SICUREZZA. QUESTO SOFTWARE NON E' ADATTO ALL'USO IN OPERAZIONI DI NAVIGAZIONE AEREA, NELLE ISTALLAZIONI NUCLEARI, NEI SISTEMI DI COMUNICAZIONE, SISTEMI DI ARMAMENTO, SISTEMI DI RESPIRAZIONE ASSISTITA DIRETTA O INDIRETTA, CONTROLLO DEL TRAFFICO AEREO O QUALUNQUE APPLICAZIONE, ISTALLAZIONE, DOVE L'ERRORE POSSA PROVOCARE MORTE, LESIONI FISICHE GRAVI, O DANNI ALLA PROPRIETA'.

CONSENT TO ELECRONIC COMMUNICATIONS. BitDefender può dover inviare avvisi legali e altre comunicazioni circa il Software e la sottoscrizione dei servizi di manutenzione o il nostro uso delle informazioni che vengono fornite ("Comunicazioni"). BitDefender invierà Comunicazioni tramite avvisi interni al prodotto o avvisi via e-mail all'indirizzo e-mail primario registrato dall'utente, oppure effettueraà Comunicazioni sui propri Siti. Con l'accettazione del presente Accordo, l'utente acconsente a ricevere tutte le Comunicazioni attraverso questi mezzi elettronici e dimostra di essere in grado di accedere alle Comunicazioni sui Siti.

AGGIORNAMENTI: accettando questo accordo, lei riconosce e accetta che il suo sistema sia utlizzato per ricevere e utilizzare aggiornamenti attraverso un protocollo peer to peer. Il protocollo non verrà utilizzato per niente altro che trasmettere e ricevere signature degli aggiornamenti BitDefender.

TECNOLOGIA DI RACCOLTA DATI- BitDefender informa che in alcuni programmi o prodotti potrebbe usare una tecnologia di raccolta dati per raccogliere informazioni tecniche (fra cui i file sospetti), per migliorare i prodotti, per fornire servizi collegati, per adattarli e per prevenire l'uso illegale o privo di licenza del prodotto o i danni causati da prodotti malware. L'Utente riconosce e accetta che BitDefender può utilizzare tali informazioni come parte dei servizi forniti relativamente al prodotto e per la prevenzione e l'arresto dell'esecuzione di programmi malware sul computer.

Accettando questo accordo, lei riconosce e accetta che la tecnologia per la sicurezza scannerizzi il suo traffico al fine di individuare eventuali malware e di prevenire i danni che questi potrebbero produrre.

L'Utente riconosce ed accetta che BitDefender possa fornire aggiornamenti e miglioramenti al programma o prodotto che vengono automaticamente scaricati sul computer.

Con l'accettazione del presente Accordo, l'Utente acconsente all'upload dei file eseguibili affinché questi possano essere scansionati dai server BitDefender. In modo simile, al fine di stabilire un contratto e di utilizzare il programma, l'utente potrebbe dover fornire a BitDefender alcuni dati personali. BitDefender informa che tratterà i dati personali in conformità con la legislazione vigente applicabile e come stabilito nelle sue Politiche sulla Privacy.

RACCOLTA DATI. L'accesso al sito web da parte dell'Utente e l'acquisto di prodotti e servizi e l'utilizzo di strumenti o contenuti tramite il sito web implicano

l'elaborazione di dati personali. Il rispetto delle normative relative all'elaborazione di dati personali, ai servizi informatici e al commercio elettronico è di assoluta importanza per BitDefender. Talvolta, per accedere ai prodotti, ai contenuti o agli strumenti l'utente dovrà in alcuni casi fornire alcune informazioni personali. BitDefender garantisce che tali dati verranno trattati confidenzialmente e in conformità alle normative relative alla protezione dei dati personali, ai servizi informatici e al commercio elettronico.

BitDefender rispetta le normative applicabili in materia di protezione dei dati ed ha compiuto i passi amministrativi e tecnici necessari a garantire la sicurezza dei dati personali che raccoglie.

L'Utente dichiara che tutti i dati forniti sono veritieri ed accurati e si impegna ad informare BitDefender di qualsiasi cambiamento di tali dati. L'Utente ha il diritto di opporsi all'elaborazione di qualsiasi dato che non sia essenziale per l'esecuzione dell'accordo e all'uso per qualsiasi scopo diverso dal mantenimento della relazione contrattuale.

Nel caso vengano forniti dettagli di terzi, BitDefender non sarà responsabile per il rispetto dei principi di informazione e di consenso, e sarà pertanto cura dell'utente garantire di aver preventivamente informato ed ottenuto il consenso dal proprietario dei dati, relativamente alla comunicazione di tali dati.

BitDefender e i suoi affiliati e partner invieranno informazioni di marketing per email o altri mezzi elettronici solo a quegli utenti che hanno acconsentito esplicitamente a ricevere comunicazioni o newsletter relative ai prodotti o servizi BitDefender.

Le politiche sulla privacy di BitDefender garantiscono all'utente il diritto di accedere, correggere, eliminare ed opporsi all'elaborazione di dati tramite avviso via e-mail all'indirizzo: juridic@bitdefender.com.

GENERALE. Questo accordo sarà regolato dalle leggi della Romania e dai regolamenti e trattati internazionali sul diritto d'autore. La giurisdizione esclusiva e la sede di decisione per qualsiasi disputa che sorga al di fuori di questi Termini di Licenza sarà in capo ai tribunali della Romania.

Nel caso di invalidità di qualsiasi previsione di questo Accordo, l'invalidità non avrà effetto sulla validità delle porzioni residue di questo Accordo.

BitDefender e i loghi BitDefender sono marchi registrati di BITDEFENDER. Tutti gli altri marchi registrati utilizzati nel prodotto o nei materiali associati sono di proprietà dei rispettivi titolari.

La licenza terminerà immediatamente senza notifica se si infrange uno qualsiasi dei suoi termini e condizioni. Non si ha diritto ad alcun rimborso da BITDEFENDER o da qualsiasi rivenditore di BitDefender come risultato della cessazione. I termini e le condizioni che riguardano la riservatezza e le restrizioni d'uso resteranno in vigore anche dopo qualsiasi cessazione.

BITDEFENDER può revisionare questi Termini in qualsiasi momento e i termini revisionati si applicheranno automaticamente alle versioni corrispondenti del Software distribuito con i termini revisionati. Se qualsiasi parte di questi Termini è giudicata nulla o non applicabile, ciò non avrà effetto sulla validità del resto dei Termini, che resteranno validi ed applicabili.

In caso di controversia o inconsistenza tra le traduzioni di questi Termini nelle altre lingue, prevarrà la versione inglese emessa da BITDEFENDER.

Contatta BITDEFENDER, al n.5 di via Fabrica de Glucoza, 72322-Sector 2, Bucarest, Romania, o al N. di Tel. : 40-21-2330780 o di Fax: 40-21-2330763, indirizzo e-mail: office@bitdefender.com.

Prefazione

Questa guida è destinata a tutti gli utenti che hanno scelto **Sicurezza Totale BitDefender 2010** come soluzione di sicurezza per il computer. Le informazioni presentate in questo manuale non sono indirizzata solo agli esperti di computer ma a chiunque sia in grado di usare Windows.

Questo manuale illustra Sicurezza totale BitDefender 2010 e il processo di installazione e configurazione. Si imparerà ad utilizzare il programma Sicurezza totale BitDefender 2010, ad aggiornarlo, testarlo e personalizzarlo, in pratica a sfruttare al meglio BitDefender.

Ti auguriamo una lettura gradevole e utile.

1. Convenzioni usate in questo manuale

1.1. Convenzioni tipografiche

Nel libro vengono usati diversi stili di testo per una leggibilità migliorata. Il loro aspetto e significato vengono presentati nella tabella sottostante.

Aspetto	Descrizione
`sample syntax`	Gli esempi sintattici vengono scritte con caratteri `monospazio`.
http://www.bitdefender.com	I link URL puntano su alcuna ubicazione esterna, su server http o ftp.
sales@bitdefender.com	Gli indirizzi e-mail vengono inseriti nel testo per informazioni sui contatti.
«Prefazione» (p. xviii)	Questo è un link interno, verso qualche ubicazione nel documento.
`filename`	File e directory (cartelle) vengono scritte con fonti `monospazio`.
option	Tutte le opzioni del prodotto vengono scritte usando caratteri in **grassetto**.
`sample code listing`	Il listato codici è scritto con caratteri `monospazio`.

1.2. Avvertenze

Le avvertenze appaiono in note di testo, segnalate graficamente, offrendo alla tua attenzione informazione addizionale relativa al paragrafo corrente.

Nota

La nota è solo una piccola osservazione. Anche se la puoi omettere, la nota può provvedere informazione di valore come una caratteristica specifica o un link verso temi relazionati.

Importante

Questa richiede la tua attenzione e non è consigliato saltarla. Solitamente facilita informazione non critica ma significante.

Avvertimento

Questa è un'informazione critica che dovresti trattare con crescente cautela. Niente di male accadrà se segui le istruzioni. Dovresti leggerlo e capirlo, perché descrive qualcosa di estremamente rischioso.

2. Struttura del manuale

Il manuale è composto da diverse parti contenenti gli argomenti importanti. Inoltre, viene anche fornito un glossario per chiarire alcuni termini tecnici.

Installazione e rimozione. Istruzioni passo passo per l'installazione di BitDefender su un personal computer. Partendo dai prerequisiti per una installazione valida, l'utente viene guidato lungo l'intero processo di installazione. Infine la procedura di rimozione viene descritta nel caso si abbia bisogno di disinstallare BitDefender.

Iniziando. Contiene tutte le informazioni necessarie a muovere i primi passi con BitDefender. Viene presentata l'interfaccia di BitDefender e le procedure per risolvere i problemi, configurare le impostazioni di base e registrare il prodotto.

Modalità intermedia. Presenta l'interfaccia Modalità Intermedia di BitDefender.

Modalità avanzata. Una descrizione dettagliata dell'interfaccia Modalità Avanzata di BitDefender. Vi spieghiamo come configurare ed utilizzare tutti i moduli di BitDefender in modo da proteggere efficacemente il vostro computer da ogni tipo di minaccia (malware, spam, hackers, contenuto inappropriato ed altro).

Integrazione in Software Windows e di terzi . Mostra come utilizzare le opzioni di BitDefender dal menu contestuale di Windows e dalla barra degli strumenti BitDefender integrata in programmi supportati di terze parti.

Come fare. Procedura per le funzioni più comuni in BitDefender

Risoluzione dei problemi e aiuto. Dove cercare e ottenere un aiuto in caso di difficoltà. E' inclusa anche una sezione FAQ (Domande frequenti).

CD di soccorso BitDefender. Descrizione del CD di soccorso BitDefender. Consente di comprendere e utilizzare le funzioni offerte da questo CD di avvio.

Glossario. Il glossario cerca di spiegare alcuni termini tecnici e poco comuni che troverai tra le pagine di questo documento.

3. Richiesta di commenti

Ti invitiamo ad aiutarci a migliorare questo manuale. Abbiamo provato e verificato tutta l'informazione con la nostra massima capacità, ma potresti trovare che le caratteristiche siano cambiate (o persino che abbiamo commesso degli errori). Per favore scrivi per parlarci su qualsiasi errore trovi in questo libro o come credi che possa essere migliorato, per aiutarci a fornirti la migliore documentazione possibile.

Facci sapere inviando una e-mail a documentation@bitdefender.com.

Importante
Per una comunicazione efficiente, vi invitiamo a scrivere i vostri documenti e le e-mails in lingua Inglese.

Installazione e rimozione

1. Requisiti del sistema

È possibile installare Sicurezza totale BitDefender 2010 solo su computer con i seguenti sistemi operativi:

- Windows XP (32/64 bit) con Service Pack 2 o superiore
- Windows Vista (32/64 bit) o Windows Vista con Service Pack 1 o successivo
- Windows 7 (32/64 bit)

Prima dell'installazione, assicurarsi che il computer soddisfa i prerequisiti hardware e software minimi.

Nota

Per verificare il sistema operativo sul computer e l'informazione hardware, fare clic con il pulsante destro del mouse su **Risorse del computer** sul desktop e quindi selezionare **Proprietà** dal menu.

1.1. Requisiti minimi di sistema

- 450 MB di spazio disponibile su disco rigido
- Processore da 800 MHz
- RAM:
  - 512 MB per Windows XP
  - 1 GB per Windows Vista/Windows 7
- Internet Explorer 6.0
- .NET Framework 1.1 (disponibile anche nel kit d'installazione)

1.2. Requisiti di sistema consigliati

- 600 MB di spazio disponibile su disco rigido
- Intel CORE Duo (1.66 GHz) o processore equivalente
- RAM:
  - 1 GB per Windows Vista/Windows 7
  - 1,5 GB per Windows Vista
- Internet Explorer 7 (o superiore)
- .NET Framework 1.1 (disponibile anche nel kit d'installazione)

1.3. Software supportato

La protezione antiphishing viene fornita solo per:

- Internet Explorer 6.0 o superiore
- Mozilla Firefox 2.5
- Yahoo Messenger 8.5
- Windows Live Messenger 8

La criptazione del Chat (IM) viene fornita solo per:

- Yahoo Messenger 8.5
- Windows Live Messenger 8

È fornita una protezione antispam per tutti i client di posta POP3/SMTP. La barra degli strumenti di BitDefender Antispam è integrata solo in:

- Microsoft Outlook 2000 / 2003 / 2007
- Microsoft Outlook Express
- Microsoft Windows Mail
- Thunderbird 2.0.0.17

2. Preparazione all'Installazione

Prima di installare BitDefender Total Security 2010, completare questi passi preliminari per assicurarsi che l'installazione funzioni senza problemi:

- Assicurarsi che il computer su cui si desidera installare BitDefender risponda ai requisiti minimi di sistema. Se il computer non risponde ai requisiti minimi di sistema, BitDefender non verrà installato o se installato non funzionerà correttamente e causerà rallentamenti e instabilità del sistema. Per un elenco completo dei requisiti di sistema, fare riferimento a «*Requisiti del sistema*» (p. 2).
- Accedere al computer utilizzando un account Amministratore.
- Rimuovere qualsiasi altro software di sicurezza dal computer. L'esecuzione simultanea di due programmi di sicurezza può influenzarne il funzionamento e causare problemi seri al sistema. Windows Defender sarà disabilitato per default prima dell'avvio dell'installazione.
- Disabilitare o rimuovere qualsiasi programma firewall che possa essere in esecuzione sul computer. L'esecuzione simultanea di due programmi firewall può influenzarne il funzionamento e causare problemi seri al sistema. Windows Firewall sarà disabilitato per default prima dell'avvio dell'installazione.

3. Installazione di BitDefender

E' possibile installare BitDefender dal CD di installazione BitDefender oppure utilizzando il file di installazione scaricato sul computer dal sito di BitDefender o da altri siti web autorizzati (ad esempio il sito web di un partner di BitDefender o un negozio on-line) Il file di installazione può essere scaricato dal sito web di BitDefender al seguente indirizzo: http://www.bitdefender.it/site/Downloads/.

- Per installare BitDefender da CD, inserire il CD nel lettore. Dopo alcuni istanti verrà visualizzata una finestra di benvenuto. Seguire le istruzioni per avviare l'installazione.

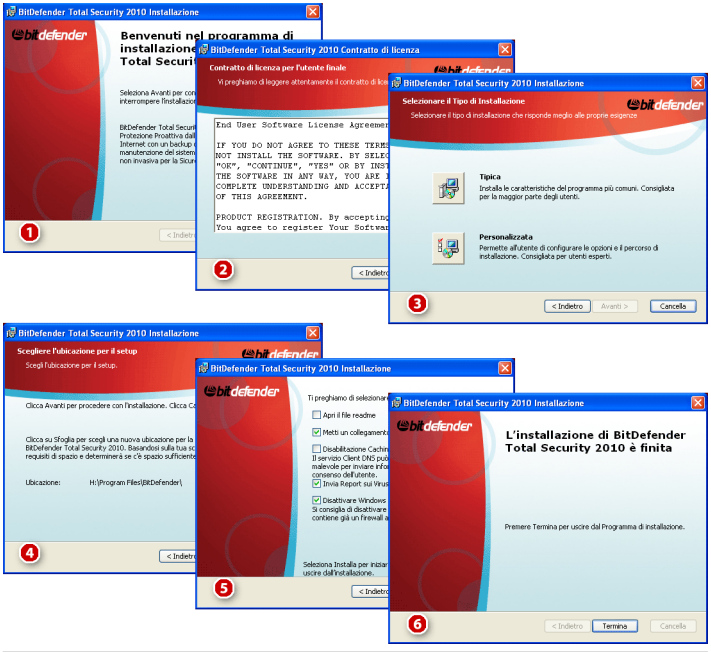
  Nota

  La schermata di benvenuto prevede l'opzione di copiare il pacchetto di installazione dal CD ad un dispositivo USB. Questo è utile se necessiti di installare BitDefender su di un PC che non possiede un drive CD (ad esempio un netbook). Inserisci il dispositivo USB nel drive USB e clicca **Copia su USB**. In seguito, spostati sul PC senza drive CD, inserisci il dispositivo USB nel drive USB e fai doppio click su `runsetup.exe` dalla cartella nella quale hai salvato il pacchetto di installazione.

  Se non appare la schermata di benvenuto, seguire questo percorso `Products\TotalSecurity\install\it\` dalla directory iniziale del CD e fare doppio clic su `runsetup.exe`.

- Per installare BitDefender utilizzando il file di installazione scaricato sul computer, individuare il file e fare doppio clic su di esso.

Il programma di installazione controllerà innanzitutto il sistema per convalidare l'installazione. Se l'installazione viene convalidata, apparirà l'assistente di setup. L'immagine seguente illustra i passaggi dell'assistente di setup.


BitDefender Total Security 2010 Installazione
Benvenuti nel programma di installazione
BitDefender Total Security 2010 Contratto di licenza
Contratto di licenza per l'utente finale
BitDefender Total Security 2010 Installazione
Selezionare il Tipo di Installazione
Tipica
Personalizzata
< Indietro
Cancella
BitDefender Total Security 2010 Installazione
Scegliere l'ubicazione per il setup
BitDefender Total Security 2010 Installazione
BitDefender Total Security 2010 Installazione
L'installazione di BitDefender Total Security 2010 è finita
Premere Termina per uscire dal Programma di installazione.
< Indietro
Termina
Cancella

Fasi per l'installazione

Seguire questi passi per installare Sicurezza Totale BitDefender 2010:

1. Selezionare **Avanti**. E' possibile annullare l'installazione in qualsiasi momento facendo clic su **Annulla**.

   Sicurezza totale BitDefender 2010 avverte se altri prodotti antivirus sono installati sul computer. Selezionare **Rimuovi** per disinstallare il corrispondente prodotto. Se si desidera continuare senza rimuovere i prodotti rilevati, selezionare **Avanti**.

   Avvertimento
   Si raccomanda di disinstallare qualsiasi altro prodotto antivirus precedentemente installato. Infatti due o più antivirus sulla stessa macchina potrebbero rendere il sistema inutilizzabile.

2. Vi preghiamo di leggere il Contratto di Licenza, e selezionare **Accetto**

   Importante
   Se non siete d'accordo con le condizioni del contratto, selezionare **Cancella**. Il processo di installazione verrà abbandonato ed uscirete dal setup.

3. Selezionare il tipo di installazione da eseguire.
   - **Tipica** - per installare il programma immediatamente, utilizzando le opzioni di installazione di default. Se si seleziona questa opzione, passare al Passo 6.
   - **Personalizzata** - per configurare le opzioni di installazione e quindi installare il programma. Questa opzione permette di modificare il percorso di installazione.
4. Per default, BitDefender Total Security 2010 verrà installato in `C:\Program Files\BitDefender\BitDefender 2010`. Se si desidera modificare il percorso d'installazione, fare clic su **Sfoglia**, quindi selezionare, la cartella dove si desidera installare Antivirus BitDefender 2010.

   Selezionare **Avanti**.
5. Selezionare le opzioni relative al processo di installazione. Le opzioni consigliate sono selezionate per default:
   - **Apri il file readme** - per aprire il file leggimi al termine dell'installazione.
   - **Collocare un collegamento sul desktop** - per collocare un collegamento a Sicurezza totale BitDefender 2010 sul desktop al termine dell'installazione.
   - **Disabilita Caching DNS** - per disabilitare il Caching DNS (Domain Name System). Il servizio Client DNS può essere utilizzato da applicazioni malevole per inviare informazioni attraverso la rete senza il consenso dell'utente.
   - **Invia Rapporti Virus** - per inviare rapporti sulla scansione antivirus al Laboratorio BitDefender per l'analisi. I report non conterranno dati confidenziali, come il vostro nome o indirizzo IP, e non verranno utilizzati per scopi commerciali.
   - **Disattiva il Firewall di Windows** - per disattivare il Firewall di Windows.

     Importante

     Raccomandiamo di disabilitare il Firewall di Windows poiché Sicurezza totale BitDefender 2010 include già un firewall avanzato. Far funzionare due firewall sullo stesso computer può causare dei problemi.

   - **Disattiva Windows Defender** - per disattivare Windows Defender; questa opzione compare slo su Windows Vista.

   Fare clic su **Installa** per avviare l'installazione. Se non è stato ancora installato, BitDefender installerà per prima .NET Framework 1.1.
6. Attendere che l'installazione sia completata e fare clic su **Termina**. Vi verrà richiesto di riavviare il sistema in modo che l'assistente di setup completi il processo di installazione. Si raccomanda di farlo al più presto.

Importante

Una volta completata l'installazione e riavviato il computer, compariranno un assistente di registrazione ed un assistente di configurazione. Eseguire questi passi per registrare e configurare Sicurezza totale BitDefender 2010 e per creare un account BitDefender.

Se sono state accettate le impostazioni di default per il percorso di installazione, è possibile vedere una nuova cartella chiamata `BitDefender` in `Program Files` che contiene la sotto-cartella `BitDefender 2010`.

3.1. Procedura guidata di Registrazione

La prima volta che avviarete il computer dopo l'installazione, comparirà l'assistente per la registrazione. L'assistente vi aiuterà a registrare BitDefender ed a configurare un conto BitDefender.

Devi creare un account per poter ricevere gli update di BitDefender. L'account BitDefender ti da accesso al supporto tecnico gratis, a offerte speciali e promozioni. Se avete perso la vostra chiave di licenza BitDefender, potete logarvi sul vostro conto in http://myaccount.bitdefender.com per recuperarla.

Nota

Se non si desidera seguire questo assitente, fare click su **Annulla**. Potete aprire la registrazione guidata in qualsiasi momento facendo click sul link **Registrazione**, situato in fondo all'interfaccia del utente.

3.1.1. Passo 1 - Registrare BitDefender Total Security 2010

BitDefender Total Security 2010
Procedura guidata di Registrazione
Registrazione BitDefender
Desidero valutare BitDefender
Desidero registrare BitDefender con una chiave di licenza
Inserire una chiave di licenza:
Codice di licenza:
Registra Ora
Non disponi di una chiave di licenza? Acquistane una ora!
Per avere maggiori informazioni su ogni opzione mostrata nell'Interfaccia Utente di BitDefender, muovere il mouse sulla finestra. Un testo di aiuto dettagliato verrà visualizzato in questa area.
Annulla
Indietro
Avanti

Registrazione

BitDefender Total Security 2010 ha un periodo di prova di 30 giorni. Per continuare a valutare il prodotto, selezionare **Voglio continuare a valutare BitDefender** e fare clic su **Avanti**.

Per registrare Sicurezza totale BitDefender 2010>

1. Selezionare **Voglio registrare BitDefender con una nuova chiave di licenza**.
2. Inserire la chiave di licenza nel campo di modifica.

Nota

Potete trovare la vostra chiave di licenza:

- sull'etichetta del CD.
- sulla scheda di registrazione del prodotto.
- sulla mail di acquisto online.

Se non si ha una chiave di licenza BitDefender, fare clic sul link fornito per andare al negozio on-line di BitDefender ed acquistare una.

3. Fare clic su **Registra Ora**.
4. Selezionare **Avanti**.

Se viene rilevata una chiave di licenza BitDefender valida sul sistema, è possibile continuare ad usare tale chiave facendo clic su **Avanti**.

3.1.2. Passo 2 - Creare un Account BitDefender

BitDefender Total Security 2010
Procedura guidata di Registrazione
Account BitDefender:
Per gli aggiornamenti e l'assistenza, attivare BitDefender creando l'account. L'attivazione può essere rimandata di 15 gg per le versioni di prova e di 30 gg per quelle registrate. Più informazioni su http://www.bitdefender.com/why_register.
Crea un nuovo account
Indirizzo e-mail:
Inserire indirizzo e-mail
Password:
Conferma password
Reinserisci password:
Conferma password
Opzioni e-mail:
Invia tutti i messaggi
Creato il:
Accedi (account creato precedentemente)
Registra dopo (la registrazione è obbligatoria)
Per avere maggiori informazioni su ogni opzione mostrata nell'Interfaccia Utente di BitDefender, muovere il mouse sulla finestra. Un testo di aiuto dettagliato verrà visualizzato in questa area.
Annulla
Indietro
Termina

Creazione Account

Se non si desidera creare un account BitDefender al momento, selezionare **Registra più tardi** e fare clic su **Termina**. Altrimenti, procedere secondo la vostra situazione attuale:

- «Non possiedo un account BitDefender» (p. 10)
- «Ho già un account BitDefender» (p. 11)

Importante

E' necessario creare un account entro 15 giorni dall'installazione di BitDefender (se il prodotto viene registrato con una chiave di licenza, la scadenza è estesa a 30 giorni). Altrimenti, BitDefender non sarà più aggiornato.

Non possiedo un account BitDefender

Per creare correttamente un account BitDefender, seguire questi passaggi:

1. Selezionare **Crea un nuovo account**.
2. Digitare le informazioni richieste nei campi corrispondenti. I dati che fornite qui resteranno riservati.
   - **E-mail** - inserire il tuo indirizzo mail.

- **Password** - inserire una password per il vostro account BitDefender. La password deve essere lunga tra 6 e 16 caratteri.
- **Confermare Password** - inserire di nuovo la password specificata previamente.

Nota
Una volta che l'account è attivato, è possibile utilizzare l'indirizzo e-mail fornito e la password per accedere all'account all'indirizzo http://myaccount.bitdefender.com.

3. A tua scelta, BitDefender puo' informarti su offerte speciali e promozioni usando l'indirizzo mail del tuo account. Selezionare una delle opzioni disponibili dal menu:
   - **Inviatemi tutti i messaggi**
   - **Inviatemi solo i messaggi relativi ai prodotti**
   - **Non inviatemi alcun messaggio**
4. Fare clic su **Crea**.
5. Fare clic su **Termina** per completare l'assistente.
6. **Attivare l'account.** Prima di poter utilizzare l'account, è necessario attivarlo. Controllare l'e-mail e seguire le istruzioni nel messaggio e-mail inviato dal servizio di registrazione BitDefender.

Ho già un account BitDefender

BitDefender rileverà automaticamente se avete già registrato un account BitDefender sul vostro computer. In questo caso, fornire la password per l'account e fare clic su **Accedi**. Fare clic su **Termina** per completare l'assistente.

Se si dispone già di un account attivo, ma BitDefender non lo rileva, seguire questi passi per registrare il prodotto per tale account:

1. Selezionare **Accedi (account creato precedentemente)**.
2. Digitare l'indirizzo e-mail e la password per l'account nei campi corrispondenti.

Nota
Se avete dimenticato la vostra password, cliccate su **Password dimenticata?** e seguire le istruzioni.

3. A tua scelta, BitDefender puo' informarti su offerte speciali e promozioni usando l'indirizzo mail del tuo account. Selezionare una delle opzioni disponibili dal menu:
   - **Inviatemi tutti i messaggi**
   - **Inviatemi solo i messaggi relativi ai prodotti**
   - **Non inviatemi alcun messaggio**
4. Fare clic su **Accedi**.
5. Fare clic su **Termina** per completare l'assistente.

3.2. Procedura guidata di Configurazione

Una volta completata la registrazione, comparirà l'assistente per la configurazione. Questo assistente permette di configurare le impostazioni principali e l'interfaccia utente di BitDefender in modo che rispondano al meglio alle vostre esigenze. Al termine dell'assistente sarà possibile aggiornare i file del prodotto e le firme dei malware ed effettuare una scansione dei file di sistema e delle applicazioni per assicurarsi che non siano infetti.

L'assistente è costituto da alcuni semplici passaggi. Il numero di passaggi dipende dalle scelte effettuate. Tutti i passaggi vengono presentati qui, ma si verrà avvisati quando le proprie scelte ne influenzano il numero.

Il completamento dell'assistente non è obbligatorio; in ogni caso vi raccomandiamo di farlo per risparmiare tempo e assicurarsi che il sistema sia sicuro ancor prima che BitDefender Total Security 2010 sia installato. Se non si desidera seguire questo assitente, fare click su **Annulla**. BitDefender vi informerà sui componenti che dovrete configurare all'apertura del interfaccia del utente.

3.2.1. Passo 1 - Selezione del Profilo di Utilizzo

BitDefender Total Security 2010
Procedura guidata di configurazione BitDefender
Benvenuto alla procedura guidata di configurazione BitDefender!
Questo assistente permetterà di configurare le impostazioni e l'interfaccia utente di BitDefender in modo da rispondere ai propri requisiti.
Selezionare l'opzione che meglio si addice al modo in cui viene utilizzato il PC.
Tipica
Padre
Giocatore
Personalizzato
Questo PC viene utilizzato per navigare su Internet e per attività multimediali.
Questo PC viene utilizzato da un bambino.
Questo PC viene utilizzato principalmente per giocare.
Configurazione BitDefender personalizzata.
Per avere maggiori informazioni su ogni opzione mostrata nell'Interfaccia Utente di BitDefender, muovere il mouse sulla finestra. Un testo di aiuto dettagliato verrà visualizzato in questa area.
Annulla
Indietro
Avanti

Profili di Utilizzo

Fare clic sul pulsante che descrive al meglio le attività compiute sul computer (il profilo di utilizzo).

Opzione	Descrizione
Tipico	Fare clic qui se il PC è utilizzato principalmente per navigare e per attività multimediali.
Genitore	Fare clic qui se il PC è utilizzato da bambini e si desidera controllarne l'accesso ad Internet utilizzando il modulo Controllo Genitori.
Giocatore	Fare clic qui se il PC è utilizzato principalmente per giocare.
Personalizzato	Fare clic qui se si desiderano configurare tutte le impostazioni principali di BitDefender.

Il profilo di utilizzo può essere reimpostato in un secondo momento dall'interfaccia del prodotto.

3.2.2. Passo 2 - Descrivere il Computer

BitDefender Total Security 2010
Procedura guidata di configurazione BitDefender
Scegliere quali di queste opzioni valgono per questo PC
Questo passo consente di configurare la Gestione rete domestica BitDefender e la Modalità portatile BitDefender. Selezionare le caselle che si addicono alla descrizione di questo PC.
Questo computer si trova in una rete domestica
Selezionare questa opzione se si desidera avere un facile accesso d'interfaccia utente al modulo Gestione Rete Domestica. Questo modulo consente di gestire altri prodotti BitDefender presenti nella rete domestica, in remoto.
Questo computer è un notebook
Selezionare questa opzione se si vuole abilitare la Modalità Laptop per default. Questa modalità assicura che la batteria del laptop durerà più a lungo non eseguendo attività che richiedono alimentazione aggiuntiva.
Per avere maggiori informazioni su ogni opzione mostrata nell'Interfaccia Utente di BitDefender, muovere il mouse sulla finestra. Un testo di aiuto dettagliato verrà visualizzato in questa area.
Annulla
Indietro
Avanti

Descrizione del Computer

Selezionare le opzioni che si applicano al computer:

- **Questo computer si trova in una rete domestica.** Selezionare questa opzione se si desidera gestire il prodotto BitDefender installato sul computer da remoto (da un altro computer). Un ulteriore passaggio dell'assistente permetterà la configurazione del modulo di Gestione della Rete Domestica.

- **Questo computer è un notebook.** Selezionare questa opzione se si desidera che la Modalità Laptop sia abilitata per default. Nella Modalità portatile, le attività di scansione e backup programmate non vengono eseguite, poiché richiedono più risorse di sistema e, implicitamente, un consumo di energia superiore.

Selezionare **Successivo** per continuare.

3.2.3. Passo 3 - Selezionare l'Interfaccia Utente

BitDefender Total Security 2010
Procedura guidata di configurazione BitDefender
Scegliere il tipo di utente che meglio si addice alle proprie esigenze
Questo passaggio permette di impostare come si desidera che funzioni BitDefender e il livello di controllo che si desidera avere sulle azioni del prodotto. Scegliere l'opzione che meglio risponde ai propri requisiti.
Inesperto
Intermedio
Avanzata
Imposta e dimentica. Interfaccia utente minimalista. BitDefender prende tutte le decisioni al vostro posto.
Questa opzione imposterà l'interfaccia utente BitDefender su Intermedia. Sarà possibile passare all'interfaccia utente Avanzata in qualsiasi momento accedendo a Impostazioni > Cambia UI a Modalità Avanzata.
Questa opzione imposterà l'interfaccia utente BitDefender su Avanzata. Sarà possibile passare all'interfaccia utente Intermedia o Inesperto qualsiasi momento accedendo a Impostazioni > Cambia UI a:
Per avere maggiori informazioni su ogni opzione mostrata nell'Interfaccia Utente di BitDefender, muovere il mouse sulla finestra. Un testo di aiuto dettagliato verrà visualizzato in questa area.
Annulla
Indietro
Avanti

Modalità di visualizzazione dell'interfaccia dell'utente.

Fare clic sul pulsante che meglio descrive le capacità informatiche dell'utente per selezionare una modalità di visualizzazione dell'interfaccia utente appropriata. È possibile selezionare visualizzazione l'interfaccia utente in base a tre diverse modalità, a seconda della propria conoscenza dei computer e di BitDefender.

Modalità	Descrizione
Modalità inesperto	Adatta per principianti e per persone che desiderano che BitDefender protegga il proprio computer e i dati senza essere tanti problemi. Questa modalità è di facile utilizzo e richiede un intervento minimo da parte dell'utente. La sola cosa da fare è risolvere i problemi indicati da BitDefender. Una facile procedura guidata aiuterà a risolvere i problemi. Inoltre è possibile compiere attività comuni quale

Modalità	Descrizione
	l'aggiornamento delle firme dei virus di BitDefender e dei file del prodotto, oppure la scansione del computer.
Modalità intermedia	Rivolta ad utenti con una conoscenza media di computer, questa modalità amplia le funzionalità presenti nella Modalità inesperto. È possibile risolvere problemi separatamente e scegliere quali problemi monitorare. Inoltre è possibile gestire in remoto prodotti BitDefender installati su computer della propria casa.
Modalità avanzata	Adatta ad utenti esperti, questa modalità consente di configurare ogni funzionalità di BitDefender. Inoltre è possibile utilizzare tutte le attività fornite per proteggere il proprio computer e i dati.

3.2.4. Passo 4 - Configurazione Controllo Genitori

Nota

Questo passaggio appare solo se si è selezionata l'opzione **Personalizzata** nel passaggio 1.

BitDefender Total Security 2010
Procedura guidata di configurazione BitDefender
Proteggi le Impostazioni del Controllo genitori
Il Controllo Genitori BitDefender consente di controllare l'accesso a Internet e ad applicazioni specifiche per i bambini.
Se si condivide lo stesso account di Windows con i bambini si dovrebbero proteggere le impostazioni con una password, per assicurarsi di essere i soli a poter evitare le regole del Controllo Genitori.
Abilita Controllo genitori
Condividi un Windows Account con altri membri della famiglia
Password impostazioni del Controllo genitori:
Reinserisci password:
Se si convidide l'account di Windows con i propri figli, si consiglia di proteggere le impostazioni di Controllo Genitori con una password in modo che queste non vengano modificate o disabilitate senza autorizzazione.
Annulla
Indietro
Avanti

Configurare Controllo dei Genitori

Il Controllo dei Genitori BitDefender vi permette di controllare l'accesso ad Internet e ad applicazioni specifiche di ogni utente che possieda un account nel sistema.

Se volete usare il Controllo dei Genitori, seguire questi passaggi:

1. Selezionare **Abilita Controllo Genitori**.
2. Se si condivide il proprio account utente Windows con i bambini, selezionare la casella di controllo corrispondente e digitare la password nei campi corrispondenti in modo da proteggere le impostazioni di Controllo Genitori. Chiunque cerchi di modificare le impostazioni di Controllo Genitori deve innanzitutto fornire la password configurata.

Selezionare **Successivo** per continuare.

3.2.5. Passo 5 - Configurazione Rete BitDefender

Nota

Questo passaggio appare solo se si è specificato che il computer è collegato ad una rete domestica al Passaggio 2.

BitDefender Total Security 2010
Procedura guidata di configurazione BitDefender
Configurazione Gestione Rete Domestica
BitDefender Total Security 2010 include la Gestione Domestica, che permette di creare una rete virtuale con tutti i computer di casa e di gestire tutti i prodotti BitDefender installati in questa rete. È possibile agire come amministratore di una rete creata dall'utente o fare parte di una rete creata e gestita da un altro computer.
Abilita Rete domestica
Password della Gestione Domestica:
Reinserisci password:
Per avere maggiori informazioni su ogni opzione mostrata nell'Interfaccia Utente di BitDefender, muovere il mouse sulla finestra. Un testo di aiuto dettagliato verrà visualizzato in questa area.
Annulla
Indietro
Avanti

Configurazione della Rete BitDefender

BitDefender vi permette di creare una rete virtuale con i computer della vostra famiglia e di gestire i prodotti BitDefender installati su questa rete.

Se vuoi che questo computer faccia parte della Rete Domestica BitDefender, segui questi passi:

1. Selezionare **Abilita Rete Domestica**.
2. Inserire la stessa password di amministratore in ogni campo di modifica. La password permette ad un amministratore di gestire questo prodotto BitDefender da un altro computer.

Selezionare **Successivo** per continuare.

3.2.6. Passo 6 - Selezionare le Attività da eseguire

BitDefender Total Security 2010
Procedura guidata di configurazione BitDefender
Proteggi il PC
Si consiglia di aggiornare BitDefender ed eseguire una scansione del sistema prima di continuare. Se si decide di ignorare queste attività, BitDefender notificherà la presenza di problemi in sospeso nel sistema al termine della procedura guidata di configurazione.
Aggiornare BitDefender e compiere una scansione veloce del sistema ora
Esegui una scansione del sistema ogni giorno alle 2 AM
Per avere maggiori informazioni su ogni opzione mostrata nell'Interfaccia Utente di BitDefender, muovere il mouse sulla finestra. Un testo di aiuto dettagliato verrà visualizzato in questa area.
Annulla
Indietro
Avanti

Selezione task

Impostare BitDefender per l'esecuzione di attività importanti per la sicurezza del sistema. Sono disponibili le seguenti opzioni:

- **Aggiorna BitDefender ed esegui una scansione veloce del sistema ora** - al passaggio successivo le firme dei virus e i file di prodotto di BitDefender verranno aggiornati per proteggere il computer contro le minacce più recenti. Inoltre, immediatamente al termine dell'aggiornamento, BitDefender effettuerà una scansione dei file nelle cartelle `Windows` e `Programmi` per assicurarsi che non siano infetti. Queste cartelle contengono file del sistema operativo e delle applicazioni installate e sono di norma le prime ad essere infettate.
- **Esegui una scansione del sistema ogni giorno alle 2** - imposta BitDefender in modo da eseguire una scansione standard del computer ogni giorno alle 2. Per modificare l'orario di esecuzione della scansione, fare clic sul menu e selezionare l'orario di inizio desiderato. Se il computer è spento quando deve essere eseguita la programmazione, l'attività verrà eseguita appena si avvia il computer.

Nota

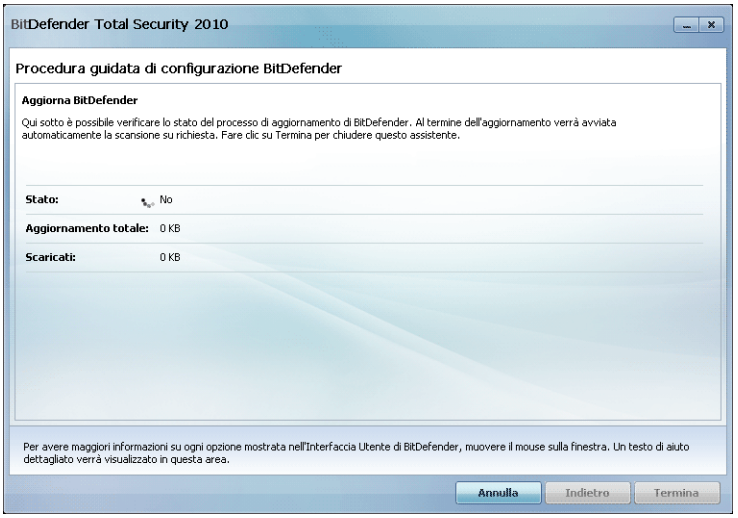
Se in un secondo momento si desidera modificare l'orario di programmazione della scansione, seguire questi passaggi:

1. Aprire BitDefender e passare l'interfaccia utente in Modalità Avanzata.
2. Clicca su **Antivirus** dal menù a sinistra.
3. Fare clic sulla scheda **Scansione Virus**.
4. Fare clic con il tasto destro sull'attività **Scansione del Sistema** e selezionare **Programma**. Apparirà una nuova finestra.
5. Cambia la frequenza e l'ora di avvio se necessario
6. Selezionare **Applica** per salvare le modifiche.

Vi raccomandiamo di abilitare queste opzioni prima di passare al passo successivo per assicurare la sicurezza del vostro sistema. Selezionare **Successivo** per continuare.

Se viene deselezionata la prima casella di controllo, non vi sono attività da eseguire nell'ultimo passaggio dell'assistente. Fare clic su **Termina** per completare l'assistente.

3.2.7. Passo 7 - Fine


BitDefender Total Security 2010
Procedura guidata di configurazione BitDefender
Aggiorna BitDefender
Qui sotto è possibile verificare lo stato del processo di aggiornamento di BitDefender. Al termine dell'aggiornamento verrà avviata automaticamente la scansione su richiesta. Fare clic su Termina per chiudere questo assistente.
Stato:
No
Aggiornamento totale:
0 KB
Scaricati:
0 KB
Per avere maggiori informazioni su ogni opzione mostrata nell'Interfaccia Utente di BitDefender, muovere il mouse sulla finestra. Un testo di aiuto dettagliato verrà visualizzato in questa area.
Annulla
Indietro
Termina

Stato dei Task

Attendere che BitDefender aggiorni le firme del malware e i motori di scansione. Non appena l'aggiornamento è completato, verrà avviata una scansione rapida del sistema. La scansione avverrà in modo silenzioso, in background. E' possibile seguire

l'icona di avanzamento della scansione nell'area di notifica. Clicca su questa icona per aprire un processo di scansione e visualizzarne il progresso.

Fare clic su **Termina** per completare l'assistente. Non devi attendere il termine della scansione

Nota

La scansione impiegherà alcuni minuti. Quando è terminata, aprire la finestra di scansione per controllare i risultati e assicurarsi che il sistema sia pulito. Se un virus è rilevato durante una scansione, dovresti aprire immediatamente BitDefender ed avviare una scansione completa

4. Upgrade

E' possibile effettuare l'aggiornamento a BitDefender Total Security 2010 se si sta utilizzando BitDefender Total Security 2010 beta oppure le versioni 2008 o 2009.

Vi sono due modi per eseguire l'aggiornamento:

- Installare BitDefender Total Security 2010 direttamente su una versione precedente. Se si installa direttamente sulla versione 2009, gli elenchi degli Amici e degli Spammer e la Quarantena verranno importati automaticamente.
- Rimuovere la versione precedente, quindi riavviare il computer e installare la nuova versione come descritto al capitolo «*Installazione di BitDefender*» (p. 5). Non verrà salvata alcuna impostazione del prodotto. Utilizzare questo metodo di aggiornamento se l'altro metodo non ha avuto successo.

5. Riparare o Rimuovere BitDefender

Se si desidera riparare o rimuovere BitDefender Total Security 2010, seguire questo percorso dal menu di avvio di Windows: **Start** → **Programmi** → **BitDefender 2010** → **Ripara o Rimuovi**.

Vi verrà richiesto di confermare la vostra scelta selezionando **Avanti**. Apparirà una nuova finestra dove potrete selezionare:

- **Riparare** - per re-installare tutte le componenti del programma installate dal setup precedente.

  Scegliendo di riparare BitDefender, la seguente nuova finestra comparirà. Selezionare **Riparare** per iniziare il processo di riparazione.

  Riavviare il computer quando richiesto, e quindi selezionare **Installa** per reinstallare Sicurezza Totale BitDefender 2010.

  Una volta completato il processo di installazione, apparirà una nuova finestra. Selezionare **Termina**.

- **Rimuovi** - per rimuovere tutte le componenti installate.

  Nota
  Vi consigliamo di scegliere **Rimuovere** per una reinstallazione pulita.

  Scegliendo di rimuovere BitDefender, apparirà una nuova finestra.

  Importante

  Rimuovendo BitDefender, non sarete più protetti da virus, spyware e hacker. Se desiderate che Windows Firewall e Windows Defender (solo su Windows Vista) vengano attivati dopo aver disinstallato BitDefender, selezionare le caselle corrispondenti.

  fare clic su **Rimuovi** per iniziare la rimozione di Sicurezza Totale BitDefender 2010 dal computer.

  Una volta completato il processo di rimozione, apparirà una nuova finestra. Selezionare **Termina**.

  Nota
  Al termine del processo di disinstallazione, consigliamo di cancellare la cartella `BitDefender` dei `Program Files`.

Iniziando

6. Panoramica

Una volta che avrete installato BitDefender il vostro computer sarà protetto. Se non hai completato la procedura di assistenza, devi aprire BitDefender e correggere eventuali errori. Devi configurare i componenti di BitDefender o prendere azioni preventive per proteggere i tuoi computer e i tuoi dati Se lo desideri, puoi fare in modo che Bitdefender non ti allerti per determinati problemi.

Se non hai registrato il prodotto (e/o non hai creato un account BitDefender) ricorda di farlo prima che il periodo di prova finisca. E' necessario creare un account entro 15 giorni dall'installazione di BitDefender (se il prodotto viene registrato con una chiave di licenza, la scadenza è estesa a 30 giorni). Altrimenti, BitDefender non sarà più aggiornato. Per ulteriori informazioni sulla registrazione, ti preghiamo di riferirti a «*Registrazione e Il mio Account*» (p. 52).

6.1. Apertura di BitDefender in corso

Per accedere all'interfaccia principale di Sicurezza totale BitDefender 2010, usare il menu Start di Windows, seguendo il percorso: **Start → Tutti i programmi → BitDefender 2010 → Sicurezza totale BitDefender 2010** o più rapidamente facendo doppio clic sull'icona BitDefender presente nella barra delle applicazioni.

6.2. Modalità di visualizzazione dell'interfaccia dell'utente.

Sicurezza totale BitDefender 2010 soddisfa le esigenze di persone esperte e di principianti. L'interfaccia grafica dell'utente è quindi stata progettata per essere adatta a qualsiasi categoria di utenti.

È possibile selezionare visualizzazione l'interfaccia utente in base a tre diverse modalità, a seconda della propria conoscenza dei computer e di BitDefender.

Modalità	Descrizione
Modalità inesperto	Adatta per principianti e per persone che desiderano che BitDefender protegga il proprio computer e i dati senza essere tanti problemi. Questa modalità è di facile utilizzo e richiede un intervento minimo da parte dell'utente. La sola cosa da fare è risolvere i problemi indicati da BitDefender. Una facile procedura guidata aiuterà a risolvere i problemi. Inoltre è possibile compiere attività comuni quale l'aggiornamento delle firme dei virus di BitDefender e dei file del prodotto, oppure la scansione del computer.

Modalità	Descrizione
Modalità intermedia	Rivolta ad utenti con una conoscenza media di computer, questa modalità amplia le funzionalità presenti nella Modalità inesperto. È possibile risolvere problemi separatamente e scegliere quali problemi monitorare. Inoltre è possibile gestire in remoto prodotti BitDefender installati su computer della propria casa.
Modalità avanzata	Adatta ad utenti esperti, questa modalità consente di configurare ogni funzionalità di BitDefender. Inoltre è possibile utilizzare tutte le attività fornite per proteggere il proprio computer e i dati.

La modalità interfaccia utente viene selezionata nella procedura guidata di configurazione. Questa procedura guidata appare dopo la procedura guidata di registrazione, la prima volta che si accede al computer dopo aver installato il prodotto. Se annulli la procedura guidata di registrazione o quella di configurazione, la modalità di interfaccia utente sarà la Modalità Intermedia per default.

Per cambiare modalità di interfaccia utente, eseguire i seguenti passi:

1. Apri BitDefender.
2. Fare clic sul pulsante **Impostazioni** in alto a destra.
3. Nella categoria Impostazioni interfaccia utente, fare clic sulla freccia sul pulsante e selezionare la modalità desiderata dal menu.
4. Fare clic su**OK** per salvare e applicare i cambiamenti.

6.2.1. Modalità inesperto

Se si è inesperti in materia di computer, l'interfaccia Modalità inesperto potrebbe essere la scelta migliore. Questa modalità è semplice da utilizzare e richiede pochissimo intervento da parte dell'utente.

Modalità inesperto

La finestra è suddivisa in quattro sezioni principali:

- **Stato della sicurezza** informa in merito ai problemi che riguardano la sicurezza del computer e aiuta a risolverli. Facendo clic su **Risolvi tutti i problemi**, una procedura guidata aiuterà a risolvere facilmente minacce alla sicurezza del computer e dei dati. Per ulteriori informazioni, far riferimento a «*Risolvi i Problemi*» (p. 40).
- In **Proteggi il PC** è possibile trovare le attività che proteggono il computer e i dati. Le attività disponibili che possono essere eseguite sono diverse a seconda del profilo di utilizzo selezionato.
  - Il pulsante **Esegui scansione Ora** avvia una scansione standard del sistema alla ricerca di virus, spyware e altro malware. Appare la procedura guidata Antivirus Scan che illustra il processo di scansione. Per ulteriori informazioni sulla procedura guidata, far riferimento a «*Procedura guidata scansione antivirus*» (p. 57).
  - Il pulsante **Aggiorna Ora** permette di aggiornare le firme dei virus e i file di prodotto di BitDefender. Apparirà una nuova finestra, dove potrete visualizzare lo stato dell'aggiornamento. Se vengono rilevati degli aggiornamenti, questi vengono automaticamente scaricati ed installati sul computer.
  - Quando viene selezionato il profilo **Tipico** il pulsante **Backup** permette di effettuare il backup dei dati e ripristinarli se necessario. Fare clic sul pulsante e selezionare l'attività desiderata dal menu. Un assistente fornisce aiuto

nell'esecuzione dell'attività. Per ulteriori informazioni fare riferimento alla sezione «*Assistenti di Backup e di Ripristino*» (p. 75).

Task	Descrizione
Backup Locale	Questo assistente aiuta nel processo di creazione di un'attività di backup locale. Alla fine di questo processo sarete in grado di eseguire subito il backup dei vostri dati, o di programmare il prodotto per eseguire il backup in un secondo momento.
Ripristino Locale	Questo assistente aiuta a ripristinare i dati di cui si è effettuato il backup su un dispositivo di archiviazione locale.

- Quando è selezionato il profilo **Genitori** il pulsante **Controllo Genitori** permette di configurare le impostazioni di Controllo Genitori. Il Controllo genitori restringe le attività del computer e on-line dei vostri bambini in base alle regole definite. Le restrizioni possono includere bloccare siti web inappropriati, oltre a limitare giochi e accesso a Internet in base all'orario specificato. Per ulteriori informazioni sulla configurazione del Controllo Genitori, fare riferimento a «*Controllo genitori*» (p. 222).
- Quando viene selezionato il profilo **Giocatore** il pulsante **Attiva/disattiva Modalità Gioco** permette di attivare/disattivare la Modalità Gioco. La Modalità Gioco modifica temporaneamente le impostazioni di protezione in modo di minimizzare l'impatto sulle prestazioni del sistema.

- In **Manutenzione PC** è possibile trovare attività che ottimizzano la performance del computer e la sua velocità di risposta.
  - **Pulizia PC** permette di liberare spazio sul disco rigido e protegge la privacy cancellando i file temporanei di Internet e i cookie, i file di sistema non utilizzati e i collegamenti ai documenti recenti.
  - **Deframmentazione Disco** riorganizza i dati sul disco rigido in modo da accedere ai file più velocemente e migliorare le prestazioni complessive del sistema.
  - **Trova Duplicati** permette di trovare file aventi copie multiple sul sistema e di cancellare le copie non necessarie.
- **Profili D'uso** indica il profilo di utilizzo correntemente selezionato. Il profilo di utilizzo rispecchia le attività principali eseguite sul computer. A seconda del profilo di utilizzo, l'interfaccia del prodotto è organizzata in modo da permettere facile accesso alle attività preferite.

  Se si desidera passare ad un profilo differente oppure modificare il profilo attualmente in uso, fare clic sul profilo e seguire l'assistente di configurazione.

Nell'angolo in alto a destra della finestra è possibile vedere il pulsante **Impostazioni**. Apre una finestra in cui è possibile cambiare la modalità dell'interfaccia utente e abilitare o disabilitare le impostazioni principali di BitDefender. Per ulteriori informazioni, ti preghiamo di far riferimento a «*Configurazione delle Impostazioni fondamentali*» (p. 44).

Nell'angolo in basso a destra della finestra è possibile trovare diversi link utili.

Link	Descrizione
Compra/Rinnova	Apre una pagina web dove è possibile acquistare una chiave di licenza per il prodotto Sicurezza totale BitDefender 2010.
Registrare	Vi permette di inserire una nuova chiave di licenza o vedere la chiave di licenza attuale e lo stato della registrazione.
Supporto	Vi permette di contattare il team di supporto di BitDefender
Aiuto	Ti da accesso ad un file di aiuto che ti insegna ad usare BitDefender.
Visualizza Registri	Vi permette di visualizzare una cronologia dettagliata di tutti i task eseguiti da BitDefender nel vostro sistema.

6.2.2. Modalità intermedia

Ricolta agli utenti con una conoscenza media dei computer, la Modalità Intermedia è una interfaccia semplice che fornisce accesso a tutti i moduli di base. Si dovranno monitorare avvertimenti e avvisi critici e risolvere problemi.

BitDefender Total Security 2010
Impostazioni
DASHBOARD
SICUREZZA
OTTIMIZZATORE
ARCHIVIO FILE
RETE
Stato di Sicurezza
Profilo di Utilizzo: Personalizzato
Aggiorna ora
AVVISO: 1 problema influenza lo stato di sicurezza di questo PC.
Risolvi tutto
Informazioni sullo stato
SICUREZZA
ALLARME CRITICO - 1 problema in sospeso
OTTIMIZZATORE
NON MONITORATO - Nessuna informazione disponibile
ARCHIVIO FILE
NON MONITORATO - Nessuna informazione disponibile
RETE
NON CONFIGURATO - Questo modulo è disabilitato.
Il modulo dashboard visualizza lo stato della sicurezza del prodotto oltre a i link ai più importanti moduli di prodotti.
bitdefender
Rinnova Registra Ora Supporto Aiuto Visualizza registri

Modalità intermedia

La finestra Modalità Intermedia contiene 5 schede. La seguente tabella descrive brevemente ogni scheda. Per ulteriori informazioni, far riferimento alla parte «Modalità intermedia» (p. 124) di questo manuale.

Tab	Descrizione
Dashboard	Visualizza lo stato di sicurezza del sistema e permette di ripristinare il profilo di utilizzo.
Sicurezza	Mostra lo stato dei moduli di sicurezza (antivirus, antiphishing, firewall, antispam, criptazione chat, privacy, controllo vulnerabilità e moduli di aggiornamento) insieme ai links per le funzioni antivirus, aggiornamento e controllo vulnerabilità.
Ottimizzazione	Mostra lo stato delle caratteristiche di BitDefender disegnate per migliorare le performance del vostro computer, assieme ai link alle funzioni di ottimizzazione.
Archiviazione File	Mostra lo stato del vault dei file e dei moduli di backup, assieme ai link alle funzioni di criptazione e di backup.
Rete	Mostra la struttura della rete domestica BitDefender. Qui puoi attivare varie azioni per configurare e cgestire i prodotti BitDefender installati sulla tua rete casalinga In questo modo puoi gestire la sicurezza della tua rete di casa da una singola postazione

Nell'angolo in alto a destra della finestra è possibile vedere il pulsante **Impostazioni**. Apre una finestra in cui è possibile cambiare la modalità dell'interfaccia utente e abilitare o disabilitare le impostazioni principali di BitDefender. Per ulteriori informazioni, ti preghiamo di far riferimento a *«Configurazione delle Impostazioni fondamentali»* (p. 44).

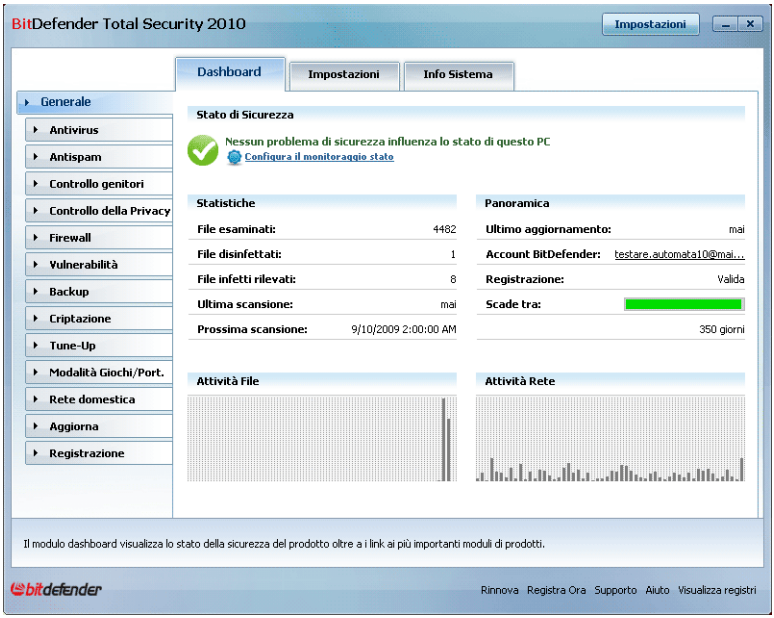
Nell'angolo in basso a destra della finestra è possibile trovare diversi link utili.

Link	Descrizione
Compra/Rinnova	Apre una pagina web dove è possibile acquistare una chiave di licenza per il prodotto Sicurezza totale BitDefender 2010.
Registrare	Vi permette di inserire una nuova chiave di licenza o vedere la chiave di licenza attuale e lo stato della registrazione.
Supporto	Vi permette di contattare il team di supporto di BitDefender
Aiuto	Ti da accesso ad un file di aiuto che ti insegna ad usare BitDefender.
Visualizza Registri	Vi permette di visualizzare una cronologia dettagliata di tutti i task eseguiti da BitDefender nel vostro sistema.

6.2.3. Modalità avanzata

La Modalità Avanzata dà accesso ad ogni specifico componente di BitDefender. Qui è possibile configurare in dettaglio BitDefender.

Nota
La Modalità Avanzata è adatta per utenti dotati di conoscenze informatiche superiori alla media, che conoscono a quali tipi di pericoli è esposto un computer e come funzionano i programmi di sicurezza.



Modalità avanzata

Sulla parte sinistra della finestra c'è un menu contenente tutti i moduli di sicurezza. Ogni modulo consiste di una o più schede che permettono la configurazione delle impostazioni di sicurezza corrispondenti oppure permettono di eseguire attività di amministrazione e di sicurezza. La seguente tabella descrive brevemente ogni modulo. Per ulteriori informazioni, far riferimento alla parte «Modalità avanzata» (p. 151) di questo manuale.

Modulo	Descrizione
Generale	Vi permette di accedere alle impostazioni generali o di visualizzare la dashboard e le informazioni dettagliate di sistema.
Antivirus	Vi permette di configurare in dettaglio il vostro scudo antivirus e le operazioni di scansione, impostare le eccezioni e configurare il modulo di quarantena.
Antispam	Permette di mantenere la cassetta postale libera da SPAM e di configurare in dettaglio le impostazioni antispam.

Modulo	Descrizione
Controllo dei Genitori	Vi permette di proteggere i vostri bambini dai contenuti inopportuni utilizzando le vostre regole di accesso al computer personalizzate.
Controllo Privacy	Vi permette di prevenire il furto di dati dal vostro computer e proteggere la vostra privacy mentre siete online.
Firewall	Consente di proteggere il computer dai tentativi di connessione non autorizzati sia in entrata che in uscita. È come una guardia al cancello – manterrà sotto controllo la connessione Internet e terrà una registrazione di chi è autorizzato ad accedere ad Internet e chi non lo è.
Vulnerabilità	Vi permette di mantenere aggiornato il software cruciale del vostro computer.
Backup	Vi consente di fare il backup dei vostri dati sul vostro computer, su dischi removibili o su una destinazione di rete per assicurare che possiate ripristinarli quando ne avrete bisogno.
Criptazione	Vi permette di criptare le comunicazioni tramite Yahoo e Windows Live (MSN) Messenger ed anche di criptare localmente i vostri file, cartelle o partizioni critiche.
Ottimizzazione	Vi consente di migliorare le performance del vostro computer tramite la deframmentazione del disco e pulizia di registri, file duplicati, etc.
Modalita' Gioco/Portatile	Vi permette di posporre i task programmati di BitDefender mentre il vostro portatile funziona con le batterie ed anche di eliminare allarmi e pop-up mentre giocate.
Rete	Vi permette di configurare e gestire diversi computer nella vostra famiglia.
Aggiornamento	Vi permette di ottenere informazioni sugli ultimi aggiornamenti, di aggiornare il prodotto e di configurare in dettaglio il processo di aggiornamento.
Registrazione	Consente di registrare Sicurezza totale BitDefender 2010, cambiare la chiave di licenza o creare un account BitDefender.

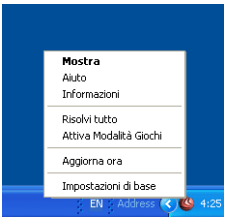
Nell'angolo in alto a destra della finestra è possibile vedere il pulsante **Impostazioni**. Apre una finestra in cui è possibile cambiare la modalità dell'interfaccia utente e abilitare o disabilitare le impostazioni principali di BitDefender. Per ulteriori informazioni, ti preghiamo di far riferimento a «*Configurazione delle Impostazioni fondamentali*» (p. 44).

Nell'angolo in basso a destra della finestra è possibile trovare diversi link utili.

Link	Descrizione
Compra/Rinnova	Apre una pagina web dove è possibile acquistare una chiave di licenza per il prodotto Sicurezza totale BitDefender 2010.
Registrare	Vi permette di inserire una nuova chiave di licenza o vedere la chiave di licenza attuale e lo stato della registrazione.
Supporto	Vi permette di contattare il team di supporto di BitDefender
Aiuto	Ti da accesso ad un file di aiuto che ti insegna ad usare BitDefender.
Visualizza Registri	Vi permette di visualizzare una cronologia dettagliata di tutti i task eseguiti da BitDefender nel vostro sistema.

6.3. Icona barra delle applicazioni

Per gestire tutto il prodotto più velocemente, è possibile utilizzare l'icona BitDefender nella barra delle applicazioni. Se si fa doppio clic su questa icona, BitDefender si aprirà. Inoltre, facendo clic con il pulsante destro sull'icona, apparirà un menu contestuale che consentirà una rapida gestione del prodotto BitDefender.



Icona della barra delle applicazioni

- **Mostra** - apre l'interfaccia di BitDefender.
- **Aiuto** - apre il file di aiuto, che spiega in dettaglio come configurare e usare Sicurezza totale BitDefender 2010.
- **Informazioni** - apre una finestra nella quale è possibile visualizzare delle informazioni su BitDefender e cercare aiuto nel caso in cui accada qualcosa di inaspettato.
- **Risolvi tutti i problemi** - aiuta a rimuovere tutte le vulnerabilità di sicurezza correnti. Se l'opzione non è disponibile, non ci sono errori da riolvere. Per ulteriori informazioni, far riferimento a «*Risolvi i Problemi*» (p. 40).
- **Modalità Gioco SI/NO** - attiva / disattiva la Modalità Gioco.
- **Aggiorna adesso** - inizia un aggiornamento immediato. Apparirà una nuova finestra, dove potrete visualizzare lo stato dell'aggiornamento.
- **Impostazioni di base** - apre una finestra dove è possibile cambiare la modalità interfaccia utente e abilitare e disabilitare il prodotto principale. Per ulteriori informazioni, far riferimento a «*Configurazione delle Impostazioni fondamentali*» (p. 44).

L'icona BitDefender nell'area di notifica fornisce informazioni relative ai problemi del computer o al funzionamento del prodotto, visualizzando un simbolo speciale come segue:

Triangolo rosso con un punto esclamativo: Si sono verificati dei problemi critici per la sicurezza del sistema. Tali problemi richiedono immediata attenzione e devono essere risolti il più presto possibile.
Lettera G: Il prodotto funziona inGame Mode.

Se BitDefender non è in funzione, l'icona nell'area di notifica è disattivata . Questo si verifica normalmente quando la licenza è scaduta. Può anche verificarsi quando i servizi di BitDefender non rispondono o quando altri errori interferiscono con il normale funzionamento di BitDefender.

6.4. Barra di Attività della Scansione

La **Barra delle attività di scansione** è una visualizzazione grafica dell'attività di scansione sul vostro sistema. Questa piccola finestra è disponibile per default solo nella Modalità Avanzata.

Le barre grigie (**Zona File**) indicano il numero di file esaminati al secondo, in una scala da 0 a 50. Le barre arancioni visualizzate nella **Zona Rete** mostrano il numero di Kbyte al secondo trasferiti (inviati e ricevuti da Internet), in una scala da 0 a 100.

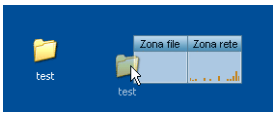
Barra di Attività della Scansione

Nota
La Barra attività di Scansione vi avviserà con una croce rossa sopra l'area corrispondente quando la protezione in tempo reale o il Firewall sono disattivati (**Zona File** o **Zona Rete**).

6.4.1. Scansiona File e Cartelle

Puoi usare la barra di scansione per scansionare velocemente files e cartelle (trascinandoli sopra alla barra) Selezionare il file o la cartella che si desidera esaminare e trascinarla sulla **Barra delle Attività di Scansione**, come nella figura seguente.

Trascinare il file



Abbandonare il file

Appare la procedura guidata Antivirus Scan che illustra il processo di scansione. Per ulteriori informazioni sulla procedura guidata, far riferimento a «*Procedura guidata scansione antivirus*» (p. 57).

Opzioni di scansione. Le opzioni di scansione sono preconfigurate per i migliori risultati di scansione. Se vengono individuati fili infetti, BitDefender cercherà di disinfettarli (rimuovere il codice malware). Se la disinfettazione non riesce, la procedura guidata Antivirus Scan consentirà di specificare altre azioni da intraprendere sui file infetti. Le opzioni di scansione sono standard e non è possibile modificarle.

6.4.2. Disabilita/ripristina la barra di attività scansione

Quando non si vuole più vedere la visualizzazione grafica, si deve semplicemente premere sulla stessa con il pulsante destro e selezionare **Nascondi**. Per ripristinare la barra delle attività di scansione, seguire questi passi:

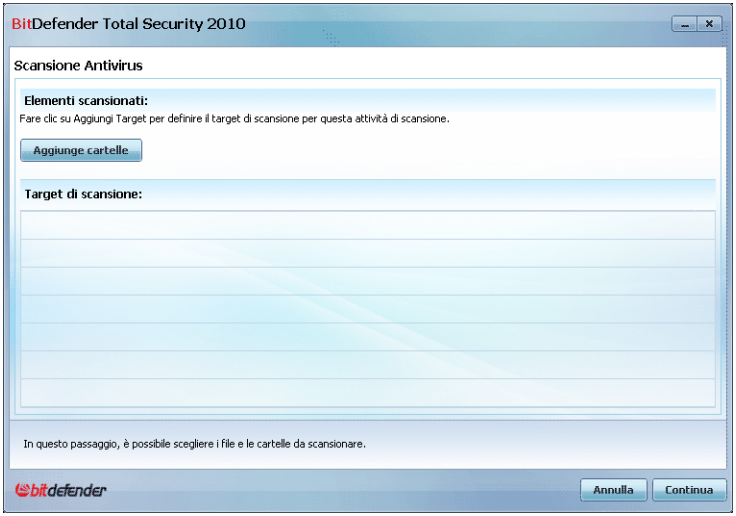
1. Apri BitDefender.
2. Fare clic sul pulsante **Impostazioni** in alto a destra.
3. Nella categoria Impostazioni generali, selezionare la casella di controllo corrispondente a **Barra Attività di Scansione**.
4. Fare clic su**OK** per salvare e applicare i cambiamenti.

6.5. Scansione Manuale di BitDefender

La scansione Manuale BitDefender consente di scansionare cartelle o partizioni di disco rigido specifiche senza dover creare una attività di scansione. Questa funzionalità è stata progettata per essere utilizzata quando Windows è in Modalità provvisoria. Se il sistema è infettato con un virus resistente, si può provare a

rimuovere il virus avviando Windows nella Modalità provvisoria e eseguendo la scansione di ogni partizione di disco rigido usando BitDefender Manual Scan.

Per accedere alla Scansione Manuale BitDefender utilizzare il menu Avvio di Windows, seguendo il percorso **Avvio → Programmi → BitDefender 2010 → Scansione Manuale di BitDefender** Apparirà la finestra seguente:


BitDefender Total Security 2010
Scansione Antivirus
Elementi scansionati:
Fare clic su Aggiungi Target per definire il target di scansione per questa attività di scansione.
Aggiunge cartelle
Target di scansione:
In questo passaggio, è possibile scegliere i file e le cartelle da scansionare.
bitdefender
Annulla
Continua

Scansione Manuale di BitDefender

Fare clic su **Aggiungi Cartella**, selezionare la posizione per cui si desidera eseguire la scansione e fare clic su **OK**. Se si desidera eseguire la scansione di cartelle multiple, ripetere questa azione per ciascuna posizione aggiuntiva.

I percorsi alle posizioni selezionate appariranno nella colonna **Target di Scansione**. Se si cambia idea circa la locazione, sarà sufficiente fare clic sul pulsante **Rimuovere** vicino. Fare clic sul pulsante **Rimuovi Tutti i Percorsi** per rimuovere tutte le posizioni aggiunte all'elenco.

Quando si ha concluso la selezione delle posizioni, fare clic su **Continua**. Appare la procedura guidata Antivirus Scan che illustra il processo di scansione. Per ulteriori informazioni sulla procedura guidata, far riferimento a «*Procedura guidata scansione antivirus*» (p. 57).

Opzioni di scansione. Le opzioni di scansione sono preconfigurate per i migliori risultati di scansione. Se vengono individuati fili infetti, BitDefender cercherà di disinfettarli (rimuovere il codice malware). Se la disinfettazione non riesce, la procedura guidata Antivirus Scan consentirà di specificare altre azioni da

intraprendere sui file infetti. Le opzioni di scansione sono standard e non è possibile modificarle.

Cos'è la Modalità provvisoria?
La modalità provvisoria è un modo speciale di avviare Windows, usato principalmente per risolvere problemi che influenzano il normale funzionamento di Windows. Tali problemi vanno da driver in conflitto a virus che impediscono a Windows di avviarsi normalmente. Nella Modalità provvisoria, Windows carica solo una parte minima di componenti del sistema operativo e dei driver fondamentali. Solo alcune applicazioni funzionano nella Modalità provvisoria. Ecco perché la maggior parte del virus sono inattivi quando si utilizza Windows nella Modalità provvisoria e perché possono essere facilmente rimossi.
Per avviare Windows nella Modalità provvisoria, riavviare il computer e premere il tasto F8 fino a quando appare il Menu opzioni avanzate di Windows. È possibile scegliere tra varie opzioni di Windows nella Modalità provvisoria. Si può selezionare **Modalità provvisoria con Networking** per abilitare l'accesso a Internet.

Nota

Per ulteriori informazioni sulla Modalità provvisoria, fare clic su Guida e Supporto tecnico di Windows (nel menu Start, fare clic su **Guida e Supporto tecnico**). È inoltre possibile trovare informazioni utili cercando su Internet.

6.6. Modalità giochi e Modalità portatile

Alcune attività del computer, ad esempio giochi o presentazioni, richiedo una maggiore risposta e performance, dal sistema e nessuna interruzione. Quando il laptop funziona a batterie, si consiglia che operazioni superflue, che consumano energia aggiuntiva, siano rimandate fino a quando il laptop è connesso all'alimentazione C/A.

Per adattarsi a queste situazioni particolari, Sicurezza totale BitDefender 2010 include due modalità operative speciali:

- Modalità giochi
- Modalità portatile

6.6.1. Modalità giochi

La Modalità Gioco modifica temporaneamente le impostazioni di protezione in modo di minimizzare l'impatto sulle prestazioni del sistema. Mentre siete in Modalità Gioco, verranno applicate le seguenti impostazioni:

- Minimizzare il consumo di memoria e di tempo del processore.
- Posporre scansioni ed aggiornamenti automatici.
- Eliminare tutti gli allarmi ed i pop-up.
- Eseguire la scansione solo dei file più importanti.

Mentre siete in Modalità Gioco, potete vedere la lettera G sull' icona BitDefender.

Uso della Modalità Gioco.

Di default, BitDefender entra automaticamente in Modalità Gioco quando iniziate un gioco incluso nella lista BitDefender dei giochi conosciuti o quando un'applicazione passa a schermo pieno. BitDefender tornerà automaticamente alla modalità normale quando si chiude il gioco o quando l'applicazione rilevata esce dallo schermo intero.

Se si vuole attivare manualmente la Modalità giochi, utilizzare uno dei metodi seguenti:

- fare clic con il pulsante destro sull'icona di BitDefender nella barra di sistema e selezionare **Attivare Modalità giochi**.
- Premere `Ctrl+Shift+Alt+G` (la hotkey di default).

Importante

Non dimenticare di disattivare la Modalità Gioco quando avete finito. Per farlo, utilizzare gli stessi metodi usati per attivarla.

Modifica Hotkey della Modalità Gioco.

Per modificare la hotkey, seguire questi passaggi:

1. Aprire BitDefender e passare l'interfaccia utente in Modalità Avanzata.
2. Fare clic su **Modalità giochi / portatile** nel menu a sinistra.
3. Fare clic sulla scheda **Modalità giochi**.
4. Fare clic sul pulsante **Impostazioni Avanzate**.
5. Sotto l'opzione **Usare HotKey**, impostare la hotkey desiderata:
   - Scegliere i tasti di modifica che si vogliono usare selezionando uno dei seguenti: tasto Control (`Ctrl`), tasto Maiuscola (`Shift`) o tasto Alternare (`Alt`).
   - Nel campo editabile, inserire la lettera corrispondente al tasto regolare che si vuole usare.

   Ad esempio, se volete usare la hotkey `Ctrl+Alt+D`, dovete solo controllare i tasti `Ctrl` e `Alt` ed inserire la `D`.

   Nota

   Togliere lo spunto da **Usare HotKey** disabiliterà la hotkey.

6. Selezionare **Applica** per salvare le modifiche.

6.6.2. Modalità Portatile

La Modalità Portatile è stata specialmente disegnata per chi usa i laptop/notebook. Il suo proposito è minimizzare l'impatto di BitDefender sul consumo di energia mentre questi apparecchi funzionino con la batteria. Nella Modalità portatile, le attività di scansione e backup programmate non vengono eseguite, poiché richiedono più risorse di sistema e, implicitamente, un consumo di energia superiore.

BitDefender rileva quando il vostro portatile sta funzionando con la batteria ed automaticamente va in Modalità Portatile. Nello stesso modo, BitDefender uscirà automaticamente dalla Modalità Portatile quando rileverà che il portatile non sta più lavorando con la batteria.

Per utilizzare la Modalità portatile, è necessario specificare nella procedura guidata di configurazione che si sta utilizzando un laptop. Se non si è selezionata l'opzione appropriata quando si eseguiva la procedura guidata, è possibile abilitare la Modalità portatile successivamente nel seguente modo:

1. Apri BitDefender.
2. Fare clic sul pulsante **Impostazioni** in alto a destra.
3. Nella categoria Impostazioni generali, selezionare la casella di controllo corrispondente a **Individuazione Modalità portatile**.
4. Fare clic su**OK** per salvare e applicare i cambiamenti.

6.7. Rilevamento dispositivo automatico

BitDefender rileva automaticamente quando si collega un dispositivo rimovibile al computer e chiede di eseguirne la scansione prima che si acceda ai suoi file. Questa operazione è consigliata per impedire che virus e altri malware infettino il computer.

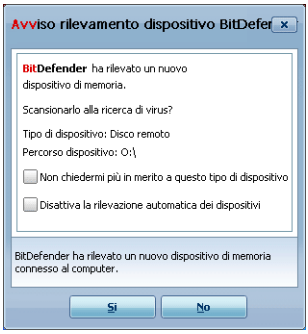
I dispositivi rilevati rientrano in una di queste categorie:

- CD/DVD
- Dispositivi di archiviazione USB, ad esempio chiavette e dischi rigidi esterni
- unità di rete (remote) mappate

Quando un tale dispositivo viene rilevato, viene visualizzata una finestra di avviso.

Per scansionare il dispositivo di archiviazione, è sufficiente fare clic su **Sì**. Appare la procedura guidata Antivirus Scan che illustra il processo di scansione. Per ulteriori informazioni sulla procedura guidata, far riferimento a «*Procedura guidata scansione antivirus*» (p. 57).

Se non si desidera scansionare il dispositivo, si deve fare clic su **No**. In questo caso, si possono ritenere utili una di queste opzioni:


Avviso rilevamento dispositivo BitDefer
BitDefender ha rilevato un nuovo dispositivo di memoria.
Scansionarlo alla ricerca di virus?
Tipo di dispositivo: Disco remoto
Percorso dispositivo: O:\
Non chiedermi più in merito a questo tipo di dispositivo
Disattiva la rilevazione automatica dei dispositivi
BitDefender ha rilevato un nuovo dispositivo di memoria connesso al computer.
Sì
No

Allarme Rilevamento Dispositivi

- **Non farmi più domande su questo tipo di dispositivo** - BitDefender non chiederà più di eseguire la scansione di dispositivi di questo tipo quando sono collegati al tuo computer.
- **Disabilita rilevamento automatico dispositivi** - Non verrà più chiesto di eseguire la scansione di nuovi dispositivi di archiviazione quando sono collegati al computer.

Se per sbaglio si disabilita il rilevamento automatico dei dispositivi di archiviazione e si desidera abilitarlo, o se si desidera configurarne le impostazioni, eseguire questi passi:

1. Aprire BitDefender e passare l'interfaccia utente in Modalità Avanzata.
2. Fare clic su **Antivirus>Virus Scan**.
3. Nell'elenco delle attività di scansione, individuare l'attività **Scansione rilevamento dispositivi**.
4. Fare clic sull'attività e selezionare **Apri**. Apparirà una nuova finestra.
5. Sulla scheda **Panoramica**, configurare le opzioni di scansione come necessarie. Per ulteriori informazioni, vi preghiamo di riferirvi a «*Configurazione delle Impostazioni di Scansione*» (p. 177).
6. Sulla scheda **Rilevamento**, scegliere i tipi di dispositivi di archiviazione da rilevare.
7. Fare clic su**OK** per salvare e applicare i cambiamenti.

7. Risolvi i Problemi

BitDefender utilizza un sistema di identificazione dei problemi per rilevare e fornire informazioni relative ai problemi che potrebbero avere effetto sulla sicurezza del computer e dei dati. Per default il sistema controlla solo una serie di problemi considerati molto importanti. Tuttavia è possibile configurare il sistema come si desidera, scegliendo di quali problemi specifici si desidera ricevere una notifica.

I problemi in sospeso vengono notificati nel modo seguente:

- Viene visualizzato un simbolo speciale sull'icona BitDefender nell'area di notifica ad indicare la presenza di problemi in sospeso.

  Triangolo rosso con un punto esclamativo: Si sono verificati dei problemi critici per la sicurezza del sistema. Tali problemi richiedono immediata attenzione e devono essere risolti il più presto possibile.

  Inoltre muovendo il cursore sull'icona un pop-up confermerà l'esistenza di problemi in sospeso.

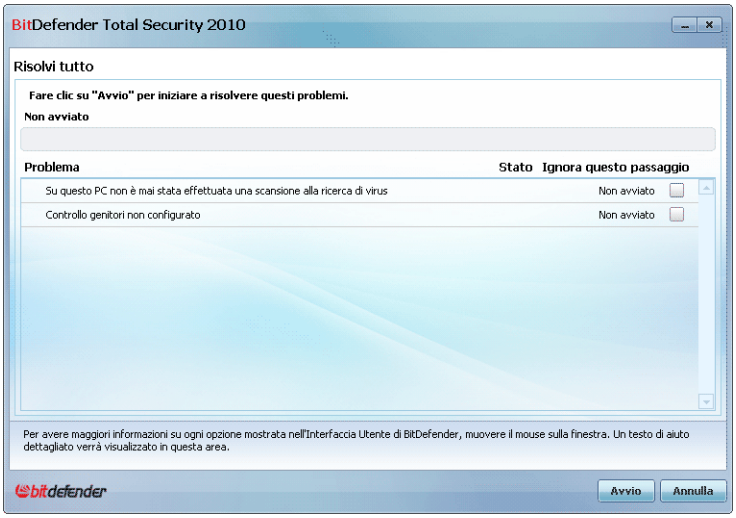
- Quando viene aperto BitDefender, l'area Stato della Sicurezza indicherà il numero di problemi del sistema.

  - In Modalità Intermedia, lo stato della sicurezza viene visualizzato nella scheda **Dashboard**.
  - In Modalità Avanzata, andare su **Generale>Dashboard** per controllare lo stato della sicurezza.

7.1. Assistente Risolti Tutti i Problemi

Il modo più semplice di risolvere i problemi esistenti è di seguire le istruzioni passo-passo dell'assistente **Risolvi Tutti i Problemi**. L'assistente aiuta a rimuovere con facilità qualsiasi minaccia per la sicurezza del computer e dei dati. Per aprire l'assistente, compiere una delle seguenti operazioni:

- Fare clic on il pulsante di destra sull icona BitDefender nell'area di notifica e selezionare **Risolvi Tutti i Problemi**.
- Apri BitDefender. A seconda della modalità dell'interfaccia utente, procedere come segue:
  - In Modalità Inesperto, fare clic su **Risolvi Tutti i Problemi**.
  - In Modalità Intermedia, andare alla scheda **Dashboard** e fare clic su **Risolvi Tutti i Problemi**.
  - In Modalità Avanzata, andare su **Generale>Dashboard** e fare clic su **Risolvi Tutti i Problemi**.


BitDefender Total Security 2010
Risolvi tutto
Fare clic su "Avvio" per iniziare a risolvere questi problemi.
Non avviato
Problema
Stato
Ignora questo passaggio
Su questo PC non è mai stata effettuata una scansione alla ricerca di virus
Non avviato
Controllo genitori non configurato
Non avviato
Per avere maggiori informazioni su ogni opzione mostrata nell'Interfaccia Utente di BitDefender, muovere il mouse sulla finestra. Un testo di aiuto dettagliato verrà visualizzato in questa area.
bitdefender
Avvio
Annulla

Assistente Risolti Tutti i Problemi

L'assistente visualizza l'elenco delle vulnerabilità di sicurezza esistenti sul computer.

Tutti i problemi attuali sono stati selezionati per essere risolti. Se vi è un problema che non si desidera risolvere, selezionare la casella di controllo corrispondente. In questo modo lo stato cambierà su **Ignora**.

Nota
Se non si desidera ricevere notifiche relative a particolari problemi è necessario configurare di conseguenza il sistema di controllo, come descritto alla sezione successiva.

Per risolvere i problemi selezionati, fare clic su **Avvia**. Alcuni problemi vengono risolti immediatamente. Per altri problemi verrà eseguito un assistente per poterli risolvere.

I problemi che l'assistente permette di risolvere possono essere raggruppati nelle seguenti categorie principali:

- **Impostazioni di sicurezza disabilitate.** Tali problemi vengono risolti immediatamente abilitando le rispettive impostazioni di sicurezza.
- **Attività di sicurezza preventiva che è necessario eseguire.** Un esempio di tali attività è la scansione del computer. Si consiglia di eseguire la scansione del compuer almeno una volta alla settimana. BitDefender compirà questa attività automaticamente nella maggior parte dei casi. Tuttavia se il programma di

scansione è stato modificato o non è stato completato, si riceverà un avviso relativo a questo problema.

Nel risolvere tali problemi, un assistente permette di completare con successo l'attività.

- **Vulnerabilità del sistema.** BitDefender controlla automaticamente il sistema alla ricerca di vulnerabilità e fornisce avvisi al riguardo. Le vulnerabilità di sistema includono quanto segue:
  - password deboli per gli account utente di Windows.
  - software obsoleto sul computer.
  - aggiornamenti di Windows mancanti.
  - Gli Aggiornamenti Automatici di Windows sono disabilitati.

  Quando è necessario risolvere tali problemi, viene avviato l'assistente scansione vulnerabilità. Questo assistente permette di risolvere le vulnerabilità di sistema rilevate. Per ulteriori informazioni fare riferimento alla sezione «*Procedura guidata di Controllo delle vulnerabilità*» (p. 69).

7.2. Configurazione del monitoraggio problemi

Il sistema di controllo dei problemi è preconfigurato per il monitoraggio e l'avviso relativo ai più importanti problemi che possono influenzare la sicurezza del computer e dei dati. Ulteriori problemi possono essere monitorati in base alle scelte compiute nell'assistente di configurazione (quando viene configurato il profilo di utilizzo). Oltre ai problemi monitorati per default, vi sono molti altri problemi su cui si può essere informati.

E' possibile configurare il sistema di controllo per rispondere al meglio alle proprie esigenze di sicurezza, selezionando di quali problemi specifici si desidera essere informati. Questa operazione è possibile in Modalità Intermedia o Avanzata.

- In Modalità Intermedia, il sistema di monitoraggio può essere configurato da posizioni separate. Attenersi alla seguente procedura:
  1. Andare alle schede **Sicurezza**, **Ottimizzazione** oppure **Archiviazione File**.
  2. Fare clic su **Configura stato monitoraggio**.
  3. Selezionare le caselle di controllo corrispondenti agli elementi che si desidera monitorare.

  Per ulteriori informazioni, far riferimento alla parte «Modalità intermedia» (p. 124) di questo manuale.
- In Modalità Avanzata, il sistema di monitoraggio può essere configurato da una posizione centrale. Attenersi alla seguente procedura:
  1. Fare clic su **Dashboard>Generale**.
  2. Fare clic su **Configura stato monitoraggio**.

3. Selezionare le caselle di controllo corrispondenti agli elementi che si desidera monitorare.

Per ulteriori informazioni fare riferimento al capitolo «*Dashboard*» (p. 152).

8. Configurazione delle Impostazioni fondamentali

È possibile configurare le impostazioni principali del prodotto (inclusa la modifica la modalità di visualizzazione dell'interfaccia utente) dalla finestra delle impostazioni fondamentali. Per aprirla, seguire una delle seguenti procedure:

- Aprire BitDefender e fare clic sul pulsante **Impostazioni** in alto a destra.
- Fare clic con i pulsante di destra sulla icona BitDefender nella barra delel applicazioni e selezionare **Impostazioni fondamentali**.

Nota

Per configurare in dettaglio le impostazioni del prodotto, utilizzare l'interfaccia nella Modalità Avanzata. Per ulteriori informazioni, far riferimento alla parte «Modalità avanzata» (p. 151) di questo manuale.

Impostazioni di base

Le impostazioni sono suddivise in tre categorie:

- Impostazioni interfaccia utente
- Impostazioni sulla sicurezza
- Impostazioni generali

Per applicare e salvare le modifiche apportate alla configurazione, fare clic su **OK**. Per chiudere la finestra senza salvare i cambiamenti, fare clic su **Elimina**.

8.1. Impostazioni interfaccia utente

In quest'area è possibile commutare la modalità di visualizzazione dell'interfaccia utente e ripristinare il profilo di utilizzo.

Commutazione della modalità di visualizzazione dell'interfaccia utente. Come descritto nella sezione *«Modalità di visualizzazione dell'interfaccia dell'utente.» (p. 23)*, ci sono tre modalità di visualizzazione dell'interfaccia utente. Ogni modalità di visualizzazione dell'interfaccia utente è progettata per una categoria specifica di utenti, in base alla loro conoscenza dei computer. In questo modo, l'interfaccia utente può soddisfare i requisiti di tutti i tipi di utenti, dai principianti agli esperti.

Il primo pulsante mostra la modalità di visualizzazione dell'interfaccia utente attuale. Per cambiare la modalità interfaccia utente, fare clic sulla freccia sul pulsante e selezionare la modalità desiderata dal menu.

Modalità	Descrizione
Modalità inesperto	Adatta per principianti e per persone che desiderano che BitDefender protegga il proprio computer e i dati senza essere tanti problemi. Questa modalità è di facile utilizzo e richiede un intervento minimo da parte dell'utente. La sola cosa da fare è risolvere i problemi indicati da BitDefender. Una facile procedura guidata aiuterà a risolvere i problemi. Inoltre è possibile compiere attività comuni quale l'aggiornamento delle firme dei virus di BitDefender e dei file del prodotto, oppure la scansione del computer.
Modalità intermedia	Rivolta ad utenti con una conoscenza media di computer, questa modalità amplia le funzionalità presenti nella Modalità inesperto. È possibile risolvere problemi separatamente e scegliere quali problemi monitorare. Inoltre è possibile gestire in remoto prodotti BitDefender installati su computer della propria casa.
Modalità Avanzata	Adatta ad utenti esperti, questa modalità consente di configurare ogni funzionalità di BitDefender. Inoltre è possibile utilizzare tutte le attività fornite per proteggere il proprio computer e i dati.

Reimpostazione del profilo di utilizzo. Il profilo di utilizzo rispecchia le attività principali eseguite sul computer. A seconda del profilo di utilizzo, l'interfaccia del prodotto è organizzata in modo da permettere facile accesso alle attività preferite.

Per riconfigurare il profilo di utilizzo, fare clic su **Reimposta Profilo di Utilizzo** e seguire l'assistente di configurazione.

8.2. Impostazioni di sicurezza

In questa area, è possibile abilitare o disabilitare le impostazioni del prodotto che riguardano vari aspetti della sicurezza del computer e dei dati. Lo stato attuale delle impostazioni è indicato usando una di queste icone:

Cerchio verde con un segno di spunta: L'impostazione è abilitata.
Cerchio rosso con un punto esclamativo: L'impostazione è disabilitata.

Per abilitare / disabilitare una impostazione, selezionare / deselezionare la casella di controllo **Abilita** corrispondente.

Avvertimento

Prestare molta attenzione prima di disabilitare la protezione antivirus in tempo reale, il firewall o aggiornamenti automatici. Disabilitare queste funzionalità potrebbe compromettere la sicurezza del proprio computer. Se è davvero necessario disabilitarle, ricordarsi di riabilitarle appena possibile.

È possibile trovare tutto l'elenco delle impostazioni e la relativa descrizione nella seguente tabella:

Impostazione	Descrizione
Antivirus	La protezione in tempo reale assicura che tutti i file vengano scansionati quando l'utente o un'applicazione eseguita nel sistema vi accede.
Aggiornamento automatico	L'aggiornamento automatico assicura che la versione più recente del prodotto BitDefender e i file di firma vengano scaricati ed installati automaticamente e regolarmente.
Controllo Vulnerabilità	Il controllo automatico delle Vulnerabilità assicura che il software cruciale del computer sia aggiornato.
Antispam	Antispam filtra messaggi e-mail che si ricevono, segnando posta non sollecitata e indesiderata come SPAM.
Antiphishing	L'Antiphishing rileva se una pagina web è impostata per rubare informazioni personali e avverte in tempo reale.
Controllo Identità	Il Controllo identità consente di impedire la diffusione dei propri dati personali su Internet senza il proprio consenso. Impedisce che messaggi immediati, e-mail

Impostazione	Descrizione
	o moduli web trasmettano dati definiti come privati a destinatari (indirizzi) non autorizzati.
Criptazione dell'IM	La Criptazione IM (Instant Messaging) rende sicure le conversazioni via Yahoo! Messenger e Windows Live Messenger a patto che i contatti IM usino un prodotto compatibile con BitDefender e software IM.
Controllo dei Genitori	Il Controllo genitori restringe le attività del computer e on-line dei vostri bambini in base alle regole definite. Le restrizioni possono includere bloccare siti web inappropriati, oltre a limitare giochi e accesso a Internet in base all'orario specificato.
Firewall	Il Firewall protegge il vostro computer dagli hacker e dagli attacchi esterni.
Criptazione File	La Criptazione File mantiene al sicuro i documenti mediante la criptazione in speciali unità protette. Se disabilitate la Criptazione File, tutti i file vault verranno bloccati e non potrete più accedere ai file che li contengono.

Lo stato di alcune di queste impostazioni può essere monitorato dal sistema di controllo dei problemi di BitDefender. Se viene disabilitata una impostazione controllata, BitDefender segnalerà un problema che deve essere risolto.

Se non si desidera che le impostazioni di monitoraggio disabilitate vengano indicate come problemi, è necessario configurare di conseguenza il sistema di monitoraggio. È possibile far ciò nella Modalità Intermedia o Avanzata.

- In Modalità Intermedia, il sistema di monitoraggio è configurato da posizioni separate, a seconda delle categorie di impostazioni. Per ulteriori informazioni, far riferimento alla parte «Modalità intermedia» (p. 124) di questo manuale.
- In Modalità Avanzata, il sistema di monitoraggio può essere configurato da una posizione centrale. Attenersi alla seguente procedura:
  1. Fare clic su **Dashboard>Generale**.
  2. Fare clic su **Configura stato monitoraggio**.
  3. Deselezionare la casella di spunta corrispondente alle voci che non si desidera monitorare.

  Per ulteriori informazioni fare riferimento al capitolo «*Dashboard*» (p. 152).

8.3. Impostazioni generali

In questa area, è possibile abilitare o disabilitare impostazioni che influenzano il comportamento del prodotto e l'esperienza utente. Per abilitare / disabilitare una impostazione, selezionare / deselezionare la casella di controllo **Abilita** corrispondente.

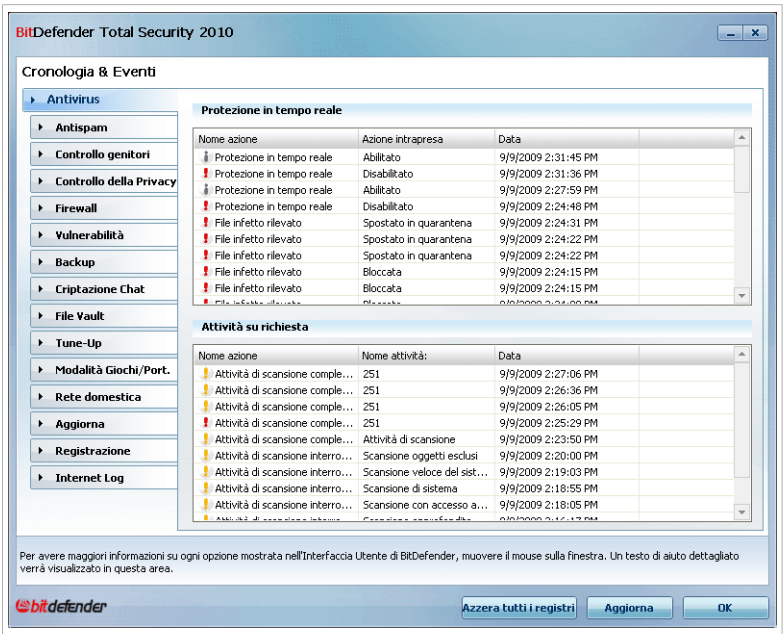
È possibile trovare tutto l'elenco delle impostazioni e la relativa descrizione nella seguente tabella:

Impostazione	Descrizione
Modalità Gioco	La Modalità giochi modifica temporaneamente le impostazioni di protezione in modo da minimizzare il loro impatto sulle performance del sistema durante le sessioni di gioco.
Rilevamento Modalità portatile	La Modalità Portatile modifica temporaneamente le impostazioni di protezione in modo da minimizzare il loro impatto sulla durata della batteria del computer portatile.
Password delle impostazioni	Questo assicura che le impostazioni di BitDefender possano essere modificate solo da una persona che conosca questa password. Quando viene abilitata questa opzione verrà richiesto di configurare la password impostazioni. Digitare la password desiderata in entrambi i campi e fare clic su **OK** per impostare la password.
Notizie BitDefender	Abilitando questa opzione, riceverete da BitDefender importanti notizie sull'azienda, aggiornamenti del prodotto e notizie sulle nuove minacce per la sicurezza.
Avvisi notifiche prodotto	Abilitando questa opzione riceverete informazioni sugli allarmi.
Barra dell'Attività di scansione	La Barra dell'attività di scansione è una piccola finestra trasparente che indica l'avanzamento dell'attività dell'attività di scansione di BitDefender. Per ulteriori informazioni, far riferimento a *«Barra di Attività della Scansione»* (p. 33).
Inviare report sui Virus	Abilitando questa opzione i report sulle scansioni antivirus verranno inviati ai Laboratori BitDefender per analisi. Questi report non contengono dati confidenziali, come il vostro nome o indirizzo IP, e non verranno usati a fini commerciali.

Impostazione	Descrizione
Rilevamento di Outbreak	Abilitando questa opzione i report riguardanti potenziali outbreak di virus verranno inviati ai Laboratori BitDefender per analisi. Questi report non contengono dati confidenziali, come il vostro nome o indirizzo IP, e non verranno usati a fini commerciali.

9. Cronologia ed Eventi

Il link **Visualizza Registri** nella parte inferiore della finestra principale di BitDefender apre un'altra finestra che visualizza la cronologia e gli eventi di BitDefender. Tale finestra offre una panoramica di tutti gli eventi relativi alla sicurezza. Ad esempio, potete controllare facilmente se l'aggiornamento è stato eseguito con successo, se è stato trovato del malware sul vostro computer, se le vostre funzioni di backup sono state eseguite senza errori, etc.


BitDefender Total Security 2010
Cronologia & Eventi
Antivirus
Antispam
Controllo genitori
Controllo della Privacy
Firewall
Vulnerabilità
Backup
Criptazione Chat
File Vault
Tune-Up
Modalità Giochi/Port.
Rete domestica
Aggiorna
Registrazione
Internet Log
Protezione in tempo reale
Nome azione | Azione intrapresa | Data
Protezione in tempo reale | Abilitato | 9/9/2009 2:31:45 PM
Protezione in tempo reale | Disabilitato | 9/9/2009 2:31:36 PM
Protezione in tempo reale | Abilitato | 9/9/2009 2:27:59 PM
Protezione in tempo reale | Disabilitato | 9/9/2009 2:24:48 PM
File infetto rilevato | Spostato in quarantena | 9/9/2009 2:24:31 PM
File infetto rilevato | Spostato in quarantena | 9/9/2009 2:24:22 PM
File infetto rilevato | Spostato in quarantena | 9/9/2009 2:24:22 PM
File infetto rilevato | Bloccata | 9/9/2009 2:24:15 PM
File infetto rilevato | Bloccata | 9/9/2009 2:24:15 PM
Attività su richiesta
Nome azione | Nome attività: | Data
Attività di scansione comple... | 251 | 9/9/2009 2:27:06 PM
Attività di scansione comple... | 251 | 9/9/2009 2:26:36 PM
Attività di scansione comple... | 251 | 9/9/2009 2:26:05 PM
Attività di scansione comple... | 251 | 9/9/2009 2:25:29 PM
Attività di scansione comple... | Attività di scansione | 9/9/2009 2:23:50 PM
Attività di scansione interro... | Scansione oggetti esclusi | 9/9/2009 2:20:00 PM
Attività di scansione interro... | Scansione veloce del sist... | 9/9/2009 2:19:03 PM
Attività di scansione interro... | Scansione di sistema | 9/9/2009 2:18:55 PM
Attività di scansione interro... | Scansione con accesso a... | 9/9/2009 2:18:05 PM
Per avere maggiori informazioni su ogni opzione mostrata nell'Interfaccia Utente di BitDefender, muovere il mouse sulla finestra. Un testo di aiuto dettagliato verrà visualizzato in questa area.
bitdefender
Azzera tutti i registri
Aggiorna
OK

Eventi

Per aiutarvi a filtrare la cronologia ed eventi di BitDefender, sulla sinistra sono disponibili le seguenti categorie:

- **Antivirus**
- **Antispam**
- **Controllo dei Genitori**
- **Controllo della Privacy**
- **Firewall**
- **Vulnerabilità**
- **Backup**
- **Criptazione IM**

- **Criptazione File**
- **Ottimizzazione**
- **Modalità portatile/giochi**
- **Rete Domestica**
- **Aggiornamento**
- **Registrazione**
- **Registro Internet**

Per ogni categoria c'è una lista di eventi disponibile. Ogni evento viene con la seguente informazione: una breve descrizione, l'azione intrapresa da BitDefender quando è successo, e la data ed ora in cui è successo. Se volete trovare ulteriori informazioni su un particolare evento della lista, cliccateci due volte sopra.

Fare clic su **Cancella tutti i registri** se si desidera rimuovere tutti i vecchi registri, oppure **Aggiorna** per assicurarsi di visualizzare i registri più recenti.

10. Registrazione e Il mio Account

BitDefender Total Security 2010 ha un periodo di prova di 30 giorni. Durante il periodo di prova il prodotto è dotato di tutte le funzionalità e può essere valutato per verificare se risponde alle vostre aspettative. Si noti che dopo 15 giorni di valutazione il prodotto cessa gli aggiornamenti a meno che non venga creato un account BitDefender. Creare un account BitDefender è parte obbligatoria del processo di registrazione

Prima del termine del periodo di prova è necessario registrare il prodotto per mantenere il computer protetto. La registrazione è una procedura in due fasi:

1. **Attivazione del prodotto (registrazione di un account BitDefender).** E' necessario creare un account BitDefender per poter ricevere gli aggiornamenti ed avere accesso all'assistenza tecnica gratuita. Se si dispone già di un account BitDefender, è possibile registrare il prodotto BitDefender con tale account. BitDefender notificherà la necessità di attivare il prodotto e aiuterà a risolvere tale problema.

   Importante

   E' necessario creare un account entro 15 giorni dall'installazione di BitDefender (se il prodotto viene registrato con una chiave di licenza, la scadenza è estesa a 30 giorni). Altrimenti, BitDefender non sarà più aggiornato.

2. **Registrazione con una chiave di licenza.** La chiave di licenza specifica la durata di tempo per cui siete autorizzati ad utilizzare il prodotto. Non appena la chiave di licenza scade BitDefender cessa di eseguire le sue funzioni e di proteggere il computer. E' necessario registrare il prodotto con una chiave di licenza valida alla scadenza del periodo di prova. E' preferibile acquistare o rinnovare una chiave di licenza alcuni giorni prima della scadenza della chiave di licenza attuale.

10.1. Registrazione Sicurezza totale BitDefender 2010

Se si desidera registrare il prodotto con una chiave di licenza oppure modificare la chiave di licenza attuale, fare clic sul link **Registra Ora** situato nella parte inferiore della finestra BitDefender. Apparirà la finestra di registrazione del prodotto.

BitDefender Total Security 2010
Procedura guidata di Registrazione
Registrazione BitDefender
Informazioni chiave di licenza attuale
Tipo: VALIDA, Utente finale
Scade tra: 350 giorni
Codice di licenza: BE089489D2B83E26D4EA
Inserire una chiave di licenza:
Codice di licenza:
Inserire una chiave di licenza
Registra Ora
Non disponi di una chiave di licenza? Acquistane una ora!
Per avere maggiori informazioni su ogni opzione mostrata nell'Interfaccia Utente di BitDefender, muovere il mouse sulla finestra. Un testo di aiuto dettagliato verrà visualizzato in questa area.
Annulla
Indietro
Termina

Registrazione

Potete vedere lo stato della registrazione BitDefender, la chiave di licenza corrente ed i giorni mancanti alla scadenza della licenza.

Per registrare Sicurezza totale BitDefender 2010>

1. Inserire la chiave di licenza nel campo di modifica.

Nota

Potete trovare la vostra chiave di licenza:

- sull'etichetta del CD.
- sulla scheda di registrazione del prodotto.
- sulla mail di acquisto online.

Se non si ha una chiave di licenza BitDefender, fare clic sul link fornito per andare al negozio on-line di BitDefender ed acquistare una.

2. Fare clic su **Registra Ora**.
3. Selezionare **Termina**.

10.2. Attivazione di BitDefender

Per attivare BitDefender, è necessario creare o accedere ad un account BitDefender. Se non si è effettuata la registrazione ad un account BitDefender durante l'assistente di registrazione iniziale, è possibile farlo nel modo seguente:

- In Modalità Inesperto, fare clic su **Risolvi Tutti i Problemi**. L'assistente permetterà di risolvere tutti i problemi in sospeso, inclusa l'attivazione del prodotto.
- In Modalità Intermedia, andare alla scheda **Sicurezza** e fare clic sul pulsante **Risolvi** corrispondente al problema relativo all'attivazione del prodotto.
- In Modalità Avanzata, andare su **Registrazione** e fare clic sul pulsante **Attiva Prodotto**.

Si aprirà la finestra di registrazione dell'account. Qui è possibile creare o accedere ad un account BitDefender per attivare il prodotto.

BitDefender Total Security 2010
Procedura guidata di Registrazione
Account BitDefender:
Per gli aggiornamenti e l'assistenza, attivare BitDefender creando l'account. L'attivazione può essere rimandata di 15 gg per le versioni di prova e di 30 gg per quelle registrate. Più informazioni su http://www.bitdefender.com/why_register.
Crea un nuovo account
Indirizzo e-mail:
Insenire indirizzo e-mail
Password:
Conferma password
Reinserisci password:
Conferma password
Opzioni e-mail:
Invia tutti i messaggi
Creato il:
Accedi (account creato precedentemente)
Registra dopo (la registrazione è obbligatoria)
Per avere maggiori informazioni su ogni opzione mostrata nell'Interfaccia Utente di BitDefender, muovere il mouse sulla finestra. Un testo di aiuto dettagliato verrà visualizzato in questa area.
Annulla
Indietro
Termina

Creazione Account

Se non si desidera creare un account BitDefender al momento, selezionare **Registra più tardi** e fare clic su **Termina**. Altrimenti, procedere secondo la vostra situazione attuale:

- «Non possiedo un account BitDefender» (p. 55)
- «Ho già un account BitDefender» (p. 55)

Importante

E' necessario creare un account entro 15 giorni dall'installazione di BitDefender (se il prodotto viene registrato con una chiave di licenza, la scadenza è estesa a 30 giorni). Altrimenti, BitDefender non sarà più aggiornato.

Non possiedo un account BitDefender

Per creare correttamente un account BitDefender, seguire questi passaggi:

1. Selezionare **Crea un nuovo account**.
2. Digitare le informazioni richieste nei campi corrispondenti. I dati che fornite qui resteranno riservati.
   - **E-mail** - inserire il tuo indirizzo mail.
   - **Password** - inserire una password per il vostro account BitDefender. La password deve essere lunga tra 6 e 16 caratteri.
   - **Confermare Password** - inserire di nuovo la password specificata previamente.

   Nota
   Una volta che l'account è attivato, è possibile utilizzare l'indirizzo e-mail fornito e la password per accedere all'account all'indirizzo http://myaccount.bitdefender.com.

3. A tua scelta, BitDefender puo' informarti su offerte speciali e promozioni usando l'indirizzo mail del tuo account. Selezionare una delle opzioni disponibili dal menu:
   - **Inviatemi tutti i messaggi**
   - **Inviatemi solo i messaggi relativi ai prodotti**
   - **Non inviatemi alcun messaggio**
4. Fare clic su **Crea**.
5. Fare clic su **Termina** per completare l'assistente.
6. **Attivare l'account.** Prima di poter utilizzare l'account, è necessario attivarlo. Controllare l'e-mail e seguire le istruzioni nel messaggio e-mail inviato dal servizio di registrazione BitDefender.

Ho già un account BitDefender

BitDefender rileverà automaticamente se avete già registrato un account BitDefender sul vostro computer. In questo caso, fornire la password per l'account e fare clic su **Accedi**. Fare clic su **Termina** per completare l'assistente.

Se si dispone già di un account attivo, ma BitDefender non lo rileva, seguire questi passi per registrare il prodotto per tale account:

1. Selezionare **Accedi (account creato precedentemente)**.
2. Digitare l'indirizzo e-mail e la password per l'account nei campi corrispondenti.

   Nota
   Se avete dimenticato la vostra password, cliccate su **Password dimenticata?** e seguire le istruzioni.

3. A tua scelta, BitDefender puo' informarti su offerte speciali e promozioni usando l'indirizzo mail del tuo account. Selezionare una delle opzioni disponibili dal menu:
   - **Inviatemi tutti i messaggi**
   - **Inviatemi solo i messaggi relativi ai prodotti**
   - **Non inviatemi alcun messaggio**
4. Fare clic su **Accedi**.
5. Fare clic su **Termina** per completare l'assistente.

10.3. Acquisto di chiavi di licenza

Se il periodo di prova è quasi in scadenza, è necessario acquistare una chiave di licenza e registrare il prodotto. Aprire BitDefender e fare clic sul link **Acquista/Rinnova**, posizionato nella parte inferiore della finestra. Il collegamento apre una pagina web dove è possibile acquistare una chiave di licenza per il prodotto BitDefender.

10.4. Rinnovo della Licenza

In quanto clienti BitDefender, avete diritto ad uno sconto quando viene rinnovata la licenza del vostro prodotto BitDefender. E' anche possibile aggiornare il prodotto alla versione più recente con uno sconto speciale o gratuitamente.

Se la chiave di licenza attuale è quasi in scadenza, è necessario rinnovare la licenza. Aprire BitDefender e fare clic sul link **Acquista/Rinnova**, posizionato nella parte inferiore della finestra. Il collegamento apre una pagina web dove è possibile rinnovare la licenza.

11. Procedure guidate

Per facilitare l'uso di BitDefender, diverse procedure guidate aiutano a svolgere specifiche attività di sicurezza o configurare impostazioni del prodotto più complesse. Questa capitolo descrive le procedure guidate potrebbero apparire quando si risolvono problemi o svolgono attività specifiche con BitDefender. Altre procedure guidate di configurazione sono descritte separatamente nella parte «Modalità avanzata» (p. 151).

11.1. Procedura guidata scansione antivirus

Ogni volta che si inizia una scansione su richiesta (ad esempio, facendo clic con il tasto destro su una cartella e selezionando **Scansiona con BitDefender**), apparirà l'assistente Scansione Antivirus BitDefender. Seguire la procedura di tre passi per completare il processo di scansione.

Nota

Se non appare la procedura guidata di scansione, potrebbe darsi che la procedura guidata sia configurata per una esecuzione sullo sfondo. Cercare l'icona di avanzamento della scansione nella barra delle applicazioni. Clicca su questa icona per aprire un processo di scansione e visualizzarne il progresso.

11.1.1. Passo 1/3 – Scansione

BitDefender inizierà la scansione degli oggetti selezionati.

Scansione in corso

Potete visualizzare lo stato della scansione e le statistiche (velocità di scansione, tempo trascorso, numero di oggetti esaminati / infetti / sospetti / nascosti ed altro).

Attendere che BitDefender finisca la scansione.

Nota
La durata del processo dipende dalla complessità della scansione.

Archivi protetti da password. Se BitDefender rileva un archivio protetto da password durante la scansione e l'azione predefinita è **Richiedi la password**, verrà chiesto di inserire la password. Gli archivi protetti da password non possono essere esaminati a meno che non forniate la password. Sono disponibili le seguenti opzioni:

- **Desidero inserire la password per questo oggetto.** Se si desidera che BitDefender scansioni l'archivio, selezionare questa opzione e digitare la password. Se non si conosce la password, scegliere un'altra opzione.
- **Non desidero inserire la password per questo oggetto (ignora questo oggetto).** Selezionare questa opzione per non scansionare questo archivio.
- **Non desidero inserire la password per questi oggetti (ignora tutti gli oggetti protetti da password).** Selezionare questa opzione se non si vuole ricevere ulteriore domande sugli archivi protetti da password. BitDefender non sarà in grado di scansionarli, ma verranno annotati nel registro della scansione.

Fare clic su **OK** per continuare la scansione.

Arresto o messa in pausa della scansione. Potete fermare la scansione in qualsiasi momento, cliccando su **Fermare**. Verrete portati all'ultimo passo dell'assistente. Per interrompere temporaneamente il processo di scansione, cliccare semplicemente su **Pausa**. Per riprendere la scansione dovrete cliccare su **Continuare**.

11.1.2. Passo 2/3 – Selezionare Azioni

Una volta completato il processo di scansione, apparirà una nuova finestra, dove potrete visualizzare i risultati della scansione.

BitDefender Total Security 2010 - Scansione approfondita del sistema
Scansione Antivirus
Sommario dei Risultati
Sotto è possibile trovare sommari di risultati per l'attività attuale di scansione.
Problemi risolti: 0
1 minacce che interessano 1 oggetto(i) richiedono attenzione.
Intraprendi un'azione generale per tutti gli elementi non risolti o seleziona individualmente l'azione per ogni elemento:
Scegli una azione:
EICAR-Test-File (not a virus)
1 problema rimanente (disinfezione fallita)
Scegli una azione:
BitDefender ha rilevato e bloccato dei virus sul computer! Questo è l'elenco delle minacce. Fare clic sul nome del virus per vedere il relativo elenco di elementi infetti.
bitdefender
Continua

Azioni

Si potrà vedere il numero di problemi che colpiscono il vs. sistema.

Gli oggetti infetti vengono mostrati in gruppi in base al malware con il quale sono stati infettati. Cliccare sul link corrispondente alla minaccia per trovare più informazioni sugli oggetti infetti.

Potete scegliere di intraprendere un'azione globale per tutti i problemi oppure selezionare azioni separate per ogni gruppo di problemi.

Una o più delle seguenti opzioni possono apparire nel menu:

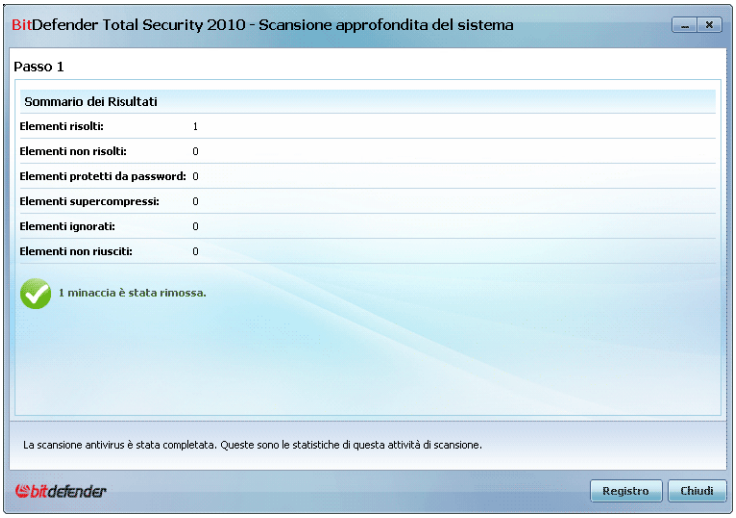
Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file rilevati. Dopo che la scansione sia stata completata, potrete aprire

Azione	Descrizione
	il log di scansione per visualizzare le informazioni su questi file.
Disinfettare	Rimuove il codice malware da file infetti.
Eliminare	Elimina i file infetti.
Sposta in quarantena	Sposta i file infetti nella quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.
Rinomina i files	Cambia il nome di file nascosti aggiungendo `.bd.ren` al loro nome. Come risultato, si potrà cercare tali file sul computer, se ve ne sono. Notare che i file nascosti non sono i file che l'utente ha nascosto in modo deliberato da Windows. Sono file nascosti da programmi speciali, noti come rootkit. I rootkit non sono file di tipo nocivo. Tuttavia sono utilizzati per rendere introvabili virus o spyware per normali programmi antivirus.

Cliccare su **Continuare** per applicare le azioni specificate.

11.1.3. Passo 3/3 – Visualizzare risultati

Quando BitDefender completa la risoluzione dei problemi, i risultati della scansione appariranno in una nuova finestra.


BitDefender Total Security 2010 - Scansione approfondita del sistema
Passo 1
Sommario dei Risultati
Elementi risolti: 1
Elementi non risolti: 0
Elementi protetti da password: 0
Elementi supercompressi: 0
Elementi ignorati: 0
Elementi non riusciti: 0
1 minaccia è stata rimossa.
La scansione antivirus è stata completata. Queste sono le statistiche di questa attività di scansione.
bitdefender
Registro
Chiudi

Riassunto

E' possibile visualizzare il sommario dei risultati. Se si desiderano informazioni esaurienti sul processo di scansione, fare clic su **Visualizza registro** per visualizzare il registro di scansione.

Importante
Se richiesto, vi preghiamo di riavviare il sistema per completare il processo di pulizia.

Cliccare su **Chiudere** per chiudere la finestra.

BitDefender potrebbe non risolvere alcuni problemi

Nella maggior parte dei casi BitDefender disinfetta con successo i file infetti che rileva o isola l'infezione. Comunque, ci sono dei problemi che non possono essere risolti.

In questi casi vi consigliamo di contattare il Team di supporto di BitDefender su www.bitdefender.it. Il nostro team di supporto vi aiuterà a risolvere i vostri problemi.

BitDefender ha rilevato dei file sospetti.

I file sospetti sono file rilevati dall'analisi euristica come potenzialmente infetti con malware la cui firma non è ancora stata rilasciata.

Se sono stati rilevati file sospetti durante la scansione, vi sarà richiesto di inviarli al Lab BitDefender. Cliccare su **OK** per inviare questi file ai laboratori BitDefender per ulteriori analisi.

11.2. Assistente Scansione Personalizzata

L'Assistente Scansione Personalizzata vi permette di creare ed eseguire un'attività di scansione personalizzata e di salvarla opzionamente come Attività Veloce quando si utilizza BitDefender in Modalità Intermedia.

Per eseguire un'attività di scansione personalizzata utilizzando l'Assistente Scansione Personalizzata, è necessario seguire questi passi:

1. In Modalità Intermedia, andare alla scheda **Sicurezza**.
2. Nell'area Funzioni Rapide, clicca **Scansione Personalizzata**.
3. Seguire i sei passi della procedura guidata per completare il processo di scansione.

11.2.1. Passo 1/6 - Finestra di Benvenuto

Questa è una finestra di benvenuto.

BitDefender Total Security 2010
Procedura guidata per la Scansione
Benvenuto
Questa Procedura guidata aiuterà a scansionare il computer alla ricerca di qualsiasi minaccia che possa colpirlo. Sarà possibile selezionare delle cartelle e/o dei file specifici da scansionare ed anche definire le azioni da intraprendere sui file infetti. Si riceverà anche un report della scansione che aiuterà a valutare il livello di sicurezza del sistema. Completare ogni passaggio e configurare il processo di scansione conformemente alle proprie necessità.
Non mostrare questo passo la prossima volta che viene eseguita la procedura guidata
bitdefender
Annulla
Avanti

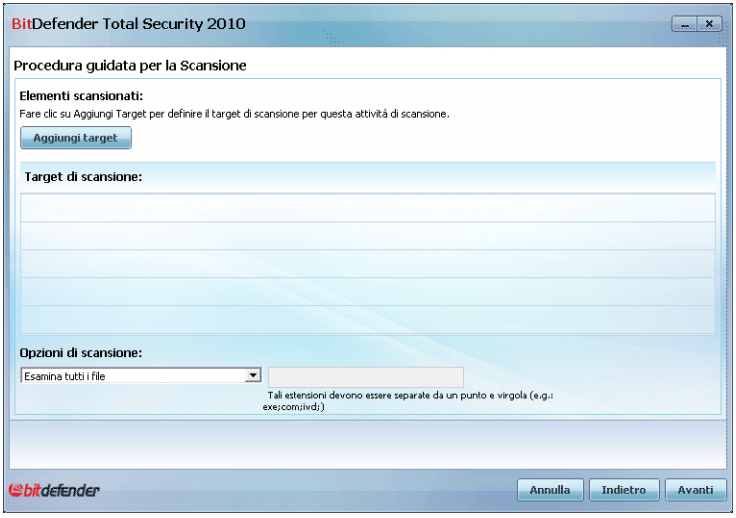
Finestra di benvenuto

Se si desidera ignorare questa finestra quando si esegue di nuovo l'assistente in futuro, selezionare la casella di controllo **Non mostrare questo passo la prossima volta che viene eseguito l'assistente**.

Selezionare **Avanti**.

11.2.2. Passo 2/6 - Selezionare Target

Qui è possibile specificare i file o le cartelle da scansionare, nonché le opzioni di scansione.


BitDefender Total Security 2010
Procedura guidata per la Scansione
Elementi scansionati:
Fare clic su Aggiungi Target per definire il target di scansione per questa attività di scansione.
Aggiungi target
Target di scansione:
Opzioni di scansione:
Esamina tutti i file
Tali estensioni devono essere separate da un punto e virgola (e.g.: exe;com;ivd;)
bitdefender
Annulla
Indietro
Avanti

Selezionare Target

Fare clic su **Aggiungere Target**, selezionare i file o le cartelle che si desidera scansionare e fare clic su **OK**. I percorsi alle posizioni selezionate appariranno nella colonna **Target di scansione**. Se si cambia idea circa la locazione, sarà sufficiente fare clic sul pulsante **Rimuovere** vicino. Fare clic sul pulsante **Rimuovi Tutto** per rimuovere tutte le posizioni aggiunte all'elenco.

Quando si è conclusa la selezione delle posizioni, impostare le **Opzioni di Scansione**. Sono disponibili le seguenti opzioni:

Opzione	Descrizione
Tutti i file	Selezionare questa opzione per esaminare tutti i file nelle cartelle desiderate.
Scansiona solo i file con estensioni di applicazione	Verranno esaminati solo i file di programma. Questo significa solo i file con le seguenti estensioni: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`;

Opzione	Descrizione
	.hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml e .nws.
Esamina solo le estensioni definite dall'utente	Verranno esaminati soltanto i file con le estensioni specificate dall'utente. Le varie estensioni devono essere separate da ";".

Selezionare **Avanti**.

11.2.3. Passo 3/6 - Selezionare Azioni

Qui è possibile specificare le impostazioni dello scanner e il livello di scansione.

Selezionare Azioni

- Selezionare le azioni da intraprendere sui file infetti e sospetti rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file infetti. Questi file appariranno nel file di rapporto.

Azione	Descrizione
Disinfetta i file	Rimuovere il codice malware dai file infetti rilevati.
Cancella i file	Cancella immediatamente i file infetti, senza alcun avviso.
Muova i files in Quarantena	Sposta i file infetti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.

- Selezionare l'azione da intraprendere sui file nascosti (rootkit). Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file nascosti. Questi file appariranno nel file di report.
Rinomina	Cambia il nome di file nascosti aggiungendo `.bd.ren` al loro nome. Come risultato, si potrà cercare tali file sul computer, se ve ne sono.

- Configurare l'aggessività dello scanner. Vi sono 3 livelli da cui scegliere. Trascinare il selettore lungo la scala per impostare il livello di protezione più adeguato:

Livello di scansione	Descrizione
Permissiva	Vengono esaminate solo le applicazioni e solo alla ricerca di virus. Il livello di consumo delle risorse è basso.
Default	Il livello di consumo delle risorse è moderato. Vengono analizzati tutti i file alla ricerca di virus e spyware.
Aggressiva	Vengono esaminati tutti i file (inclusi gli archivi) alla ricerca di virus e spyware. I file nascosti e i processi sono inclusi nella scansione. Il livello di consumo delle risorse è elevato.

Gli utenti più esperti possono trarre vantaggio dalle impostazioni di scansione offerte da BitDefender. Lo scanner può essere impostato per la ricerca di minacce malware specifiche. Questo può ridurre considerevolmente i tempi di scansione e migliorare i tempi di risposta del computer durante la scansione.

Trascinare il selettore per selezionare **Personalizzazione** quindi fare clic sul pulsante **Livello di Personalizzazione**. Apparirà una finestra. Specificare il tipo di malware per cui si desidera che BitDefender compia una scansione selezionando le opzioni appropriate:

Opzione	Descrizione
Scansione Virus	Esamina per virus conosciuti. BitDefender rileva anche virus incompleti, rimuovendo ogni possibile minaccia che possa colpire la sicurezza del vostro sistema.
Scansione adware	Esegue la scansione per minacce adware. Questi file verranno trattati come file infetti. Software che includono componenti adware potrebbero bloccarsi se questa opzione è attiva.
Scansione spyware	Esegue la scansione per minacce spyware conosciuti. Questi file verranno trattati come file infetti.
Scansiona alla ricerca di applicazioni	Cerca applicazioni legittime che possono essere usate come strumenti per spiare, per nascondere applicazioni maligne o per altri intenti maligni.
Scansione dialers	Esegue la scansione per applicazioni che utilizzano numeri di telefono a costo elevato. Questi file verranno trattati come file infetti. Software che includono componenti dialer potrebbero bloccarsi se questa opzione fosse attiva.
Scansione per i Rootkits	Esegue la scansione per oggetti nascosti (file e processi), generalmente conosciuti come rootkits.
Scansiona alla ricerca di keylogger	Scansiona applicazioni malevole che registrano i tasti premuti.

Selezionare **OK** per chiudere la finestra.

Selezionare **Avanti**.

11.2.4. Passo 4/6 - Impostazioni Aggiuntive

Prima dell'avvio della scansione sono disponibili alcune opzioni aggiuntive:

BitDefender Total Security 2010
Procedura guidata per la Scansione
Opzioni aggiuntive
Visualizza questa attività nella UI Intermedia.
Spegni il computer alla fine della scansione se non viene trovata alcuna minaccia
bitdefender
Annulla
Indietro
Inizia la Scansione

Impostazioni Aggiuntive

- Per salvare l'attività personalizzata che si sta creando per l'uso in futuro, selezionare la casella di controllo **Mostra questa attività nell'Interfaccia Utente Intermedia** ed inserire il nome dell'attività nel campo di immissione fornito.

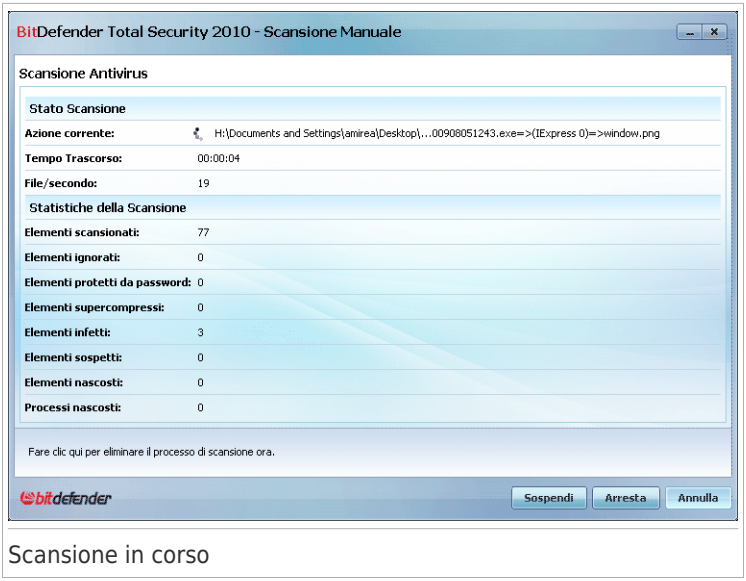
  L'attività verra aggiunta all'elenco di Attività Veloci disponibile alla scheda Sicurezza e apparirà anche in **Modalità Avanzata > Antivirus > Scansione Virus**.

- Per spegnere il computer quando la scansione è completata, selezionare la casella di controllo **Spegnere il computer quando la scansione è terminata se non sono state individuate minacce**.

Fare clic su **Avvia Scansione**.

11.2.5. Passo 5/6 - Scansione

BitDefender inizierà la scansione degli oggetti selezionati:



Scansione in corso

Nota

La durata del processo dipende dalla complessità della scansione. Facendo clic sull'icona di avanzamento della scansione nell'area di notifica si aprirà la finestra di scansione e sarà possibile osservare l'avanzamento della scansione.

11.2.6. Passo 6/6 – Visualizzare Risultati

Quando BitDefender completa il processo di scansione, i risultati della scansione verranno visualizzati in una nuova finestra:

BitDefender Total Security 2010 - Scansione Manuale
Elementi scansionati:
Sommario dei Risultati
Elementi risolti: 3
Elementi non risolti: 0
Elementi protetti da password: 0
Elementi supercompressi: 0
Elementi ignorati: 0
Elementi non riusciti: 0
3 minacce sono state rimosse.
La scansione antivirus è stata completata. Queste sono le statistiche di questa attività di scansione.
bitdefender
Registro
Chiudi

Riassunto

Viene visualizzato il riepilogo dei risultati. Se si desiderano informazioni esaurienti sul processo di scansione, fare clic su **Visualizza Registro** per visualizzare il registro di scansione.

Importante
Se richiesto, vi preghiamo di riavviare il sistema per completare il processo di pulizia.

Cliccare su **Chiudere** per chiudere la finestra.

11.3. Procedura guidata di Controllo delle vulnerabilità

L'assistente controlla le vulnerabilità del sistema e permette di risolverle.

11.3.1. Passo 1/6 – Selezionare le Vulnerabilità da controllare.

BitDefender Total Security 2010
Procedura guidata Controllo vulnerabilità BitDefender
Seleziona attività:
Questa procedura guidata identificherà le applicazioni non aggiornate e gli account di Windows che hanno una password debole. Selezionare dalla lista sottostante gli elementi da controllare per le vulnerabilità.
Controlla alla ricerca di Aggiornamenti Critici di Windows
Controlla alla ricerca di Aggiornamenti Facoltativi di Windows
Controlla gli Aggiornamenti delle Applicazioni
Controlla le Password degli Account di Windows
Configurare le impostazioni del modulo di Controllo Vulnerabilità per la seguente attività.
bitdefender
Avanti
Annulla

Vulnerabilità

Cliccare su **Avanti** per esaminare il sistema alla ricerca delle vulnerabilità selezionate.

11.3.2. Passo 2/6 - Controllare Vulnerabilità

Controllo Vulnerabilità

Attendere che BitDefender finisca il controllo alla ricerca di vulnerabilità.

11.3.3. Passo 3/6 - Aggiornare Windows

BitDefender Total Security 2010
Procedura guidata Controllo vulnerabilità BitDefender
Aggiornamenti di Windows
Rivedere tutti gli aggiornamenti trovati sotto e installarli subito o utilizzare il sistema Windows Update per scegliere quali installare.
Installa Aggiornamenti di Sistema selezionati
Controlla alla ricerca di Aggiornamenti Critici di Windows
Security Update for Microsoft .NET Framework, Version 1.1 Service Pack 1 (KB928366)
Visual Studio 2005 Service Pack 1
Security Update for Microsoft XML Core Services 4.0 Service Pack 2 (KB954430)
Security Update for Windows XP (KB971633)
Cumulative Security Update for ActiveX Killbits for Windows XP (KB973346)
Cumulative Security Update for Internet Explorer 7 for Windows XP (KB972260)
Security Update for Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package (KB973923)
Security Update for Microsoft Visual C++ 2008 Redistributable Package (KB973924)
Windows Malicious Software Removal Tool - August 2009 (KB890830)
Update for Windows XP (KB968389)
Questo è l'elenco di aggiornamenti di applicazioni Windows
bitdefender
Avanti
Annulla

Aggiornamenti di Windows

Potete vedere l'elenco degli aggiornamenti critici e non critici di Windos che non sono attualmente installati sul computer. Clicare su **Installare tutti gli aggiornamenti di sistema** per installare tutti gli aggiornamenti disponibili.

Selezionare **Avanti**.

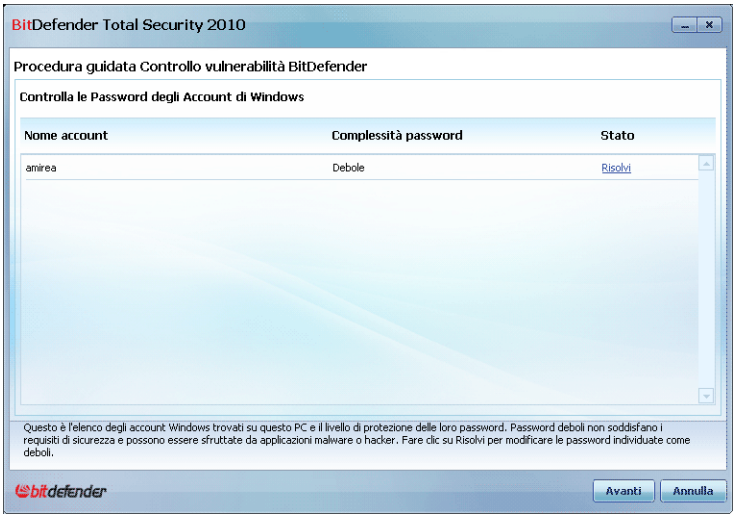
11.3.4. Passo 4/6 - Aggiornare le Applicazioni

Applicazioni

Potete vedere l'elenco di tutte le applicazioni controllate da BitDefender e se sono aggiornate. Se un'applicazione non è aggiornata, cliccare sul link fornito per scaricare la versione più recente.

Selezionare **Avanti**.

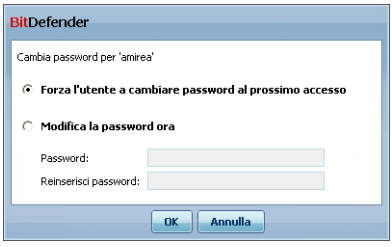
11.3.5. Passo 5/6 - Cambiare password deboli


BitDefender Total Security 2010
Procedura guidata Controllo vulnerabilità BitDefender
Controlla le Password degli Account di Windows
Nome account
Complessità password
Stato
amirea
Debole
Risolvi
Questo è l'elenco degli account Windows trovati su questo PC e il livello di protezione delle loro password. Password deboli non soddisfano i requisiti di sicurezza e possono essere sfruttate da applicazioni malware o hacker. Fare clic su Risolvi per modificare le password individuate come deboli.
bitdefender
Avanti
Annulla

Password dell'utente

Potete visualizzare l'elenco degli account di Windows configurati sul vostro computer ed il livello di protezione che le loro password forniscono. Una password può essere **forte** (difficile da indovinare) o **debole** (facile da indovinare da persone malvagie con software specializzati).

Cliccare su **Risolvere** per modificare le password deboli. Apparirà una nuova finestra.



Cambia la password

Selezionare il metodo per risolvere questo problema:

- **Forza l'utente a cambiare password al prossimo accesso.** BirDefender chiederà l'utente di cambiare la password la prossima volta che acceda a Windows.

- **Cambia password dell'utente.** Devi inserire la nuova password nei campi corrispondenti. Assicurarsi di informare l'utente in merito al cambiamento della password.

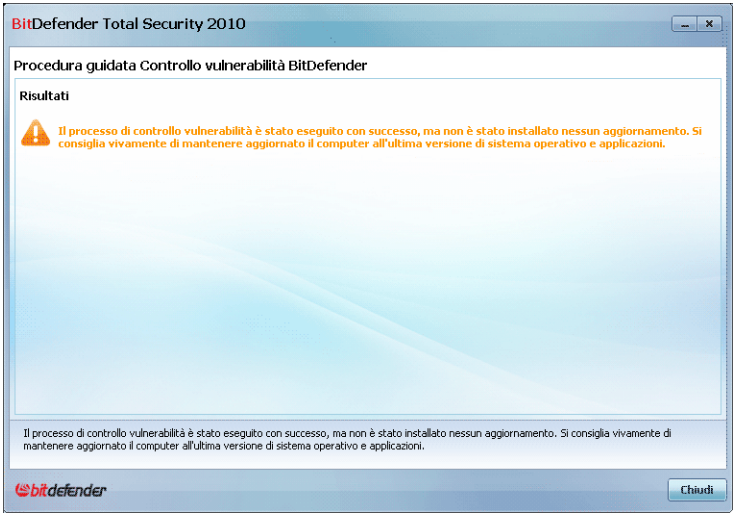
  Nota

  Per avere una password forte, utilizzare una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @). È possibile eseguire una ricerca su Internet per ulteriori informazioni e consigli sul creare forti password.

Cliccare su **OK** per cambiare la password.

Selezionare **Avanti**.

11.3.6. Passo 6/6 – Visualizzare Risultati


BitDefender Total Security 2010
Procedura guidata Controllo vulnerabilità BitDefender
Risultati
Il processo di controllo vulnerabilità è stato eseguito con successo, ma non è stato installato nessun aggiornamento. Si consiglia vivamente di mantenere aggiornato il computer all'ultima versione di sistema operativo e applicazioni.
Il processo di controllo vulnerabilità è stato eseguito con successo, ma non è stato installato nessun aggiornamento. Si consiglia vivamente di mantenere aggiornato il computer all'ultima versione di sistema operativo e applicazioni.
bitdefender
Chiudi

Risultati

Cliccare su **Chiudere**.

11.4. Assistenti di Backup e di Ripristino

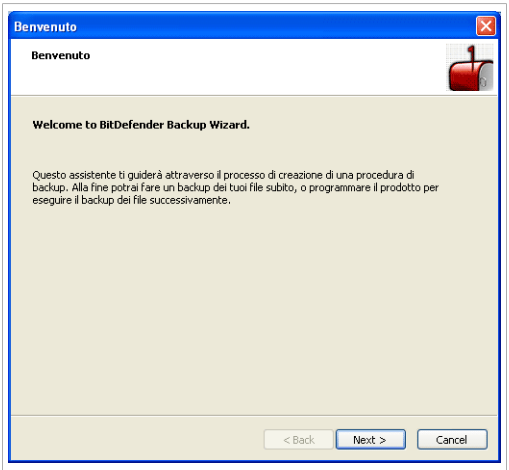
Gli assistenti di backup e di ripristino aiutano ad effettuare il backup dei dati e a ripristinarli quando necessario.

11.4.1. Assistente Backup Locale

Questo assistente aiuta nel processo di creazione di un'attività di backup locale. Alla fine di questo processo sarete in grado di eseguire subito il backup dei vostri dati, o di programmare il prodotto per eseguire il backup in un secondo momento.

Passo 1/5 - Finestra di Benvenuto

Questa è solo una pagina di benvenuto.

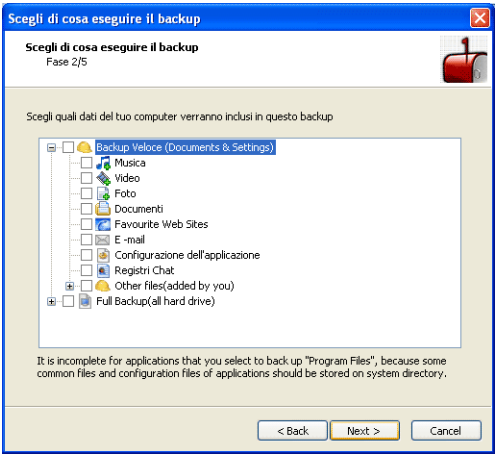

Benvenuto
Benvenuto
Welcome to BitDefender Backup Wizard.
Questo assistente ti guiderà attraverso il processo di creazione di una procedura di backup. Alla fine potrai fare un backup dei tuoi file subito, o programmare il prodotto per eseguire il backup dei file successivamente.
< Back
Next >
Cancel

Finestra di benvenuto

Selezionare **Avanti**.

Passo 2/5 - Scegliere su cosa eseguire il backup

Qui potete selezionare i dati del vostro computer su cui eseguire il backup.


Scegli di cosa eseguire il backup
Scegli di cosa eseguire il backup
Fase 2/5
Scegli quali dati del tuo computer verranno inclusi in questo backup
Backup Veloce (Documents & Settings)
Musica
Video
Foto
Documenti
Favourite Web Sites
E -mail
Configurazione dell'applicazione
Registri Chat
Other files(added by you)
Full Backup(all hard drive)
It is incomplete for applications that you select to back up "Program Files", because some common files and configuration files of applications should be stored on system directory.
< Back
Next >
Cancel

Scegli di cosa eseguire il backup

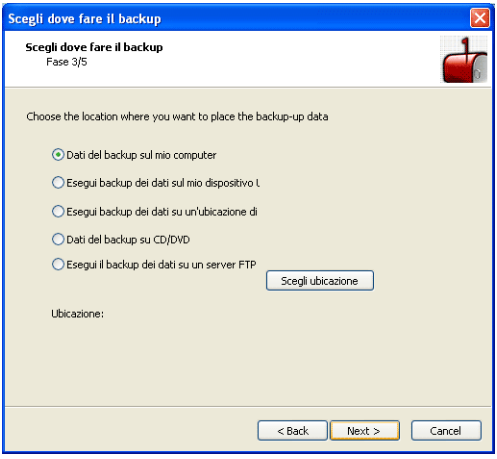
Potete scegliere tra **Backup Veloce** (musica, video, foto, email, impostazioni di applicazioni, etc.) o **Backup Completo** (tutte le partizioni).

Cliccare **Altri file**, per aggiungere altri file dal vostro desktop al **Backup Veloce**. Il **Backup Completo** può essere anche facilmente personalizzato selezionando le directory di una certa partizione sulle quali eseguire il backup.

Selezionare **Avanti**.

Passo 3/5 - Scegliere dove eseguire il backup

Qui potete selezionare l'ubicazione dei dati sui quali è stato eseguito il backup.


Scegli dove fare il backup
Scegli dove fare il backup
Fase 3/5
Choose the location where you want to place the backup-up data
Dati del backup sul mio computer
Esegui backup dei dati sul mio dispositivo U
Esegui backup dei dati su un'ubicazione di
Dati del backup su CD/DVD
Esegui il backup dei dati su un server FTP
Scegli ubicazione
Ubicazione:
< Back
Next >
Cancel

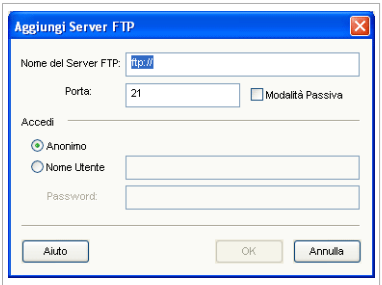
Scegli dove fare il backup

Sono disponibili le seguenti opzioni:

- **Eseguire il Backup dei dati sul mio computer**
- **Eseguire il Backup dei dati sul mio dispositivo USB**
- **Eseguire il Backup dei dati su un'ubicazione di rete**
- **Eseguire il Backup dei dati su CD/DVD**
- **Eseguire il Backup dei dati su server FTP**

Se decidete di eseguire il backup dei vostri dati sul vostro computer, dispositivo USB o un'ubicazione di rete, cliccare su **Scegliere ubicazione** e selezionare dove salvare i dati.

Se decidete di eseguire il backup dei vostri dati sul server ftp,cliccare su **Scegliere ubicazione** e selezionare dove salvare i dati (FTP). Apparirà una nuova finestra.



Aggiungi Server FTP

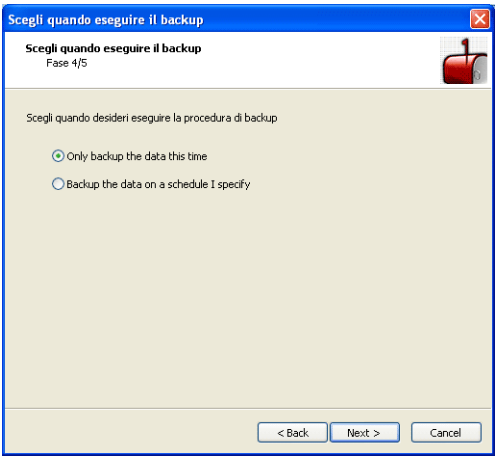
È necessario configurare il server FTP come segue:

1. Inserire il nome del FTP nel campo corrispondente.
2. Se il server FTP usa una porta diversa rispetto porta di default 21, digitare nel campo corrispondente.
3. Per utilizzare la modalità passiva (il server FTP avvia la connessione), selezionare la **modalità passiva** casella di controllo.
4. Se il server FTP consente l'accesso anonimo, è possibile lasciare il **Anonimo** opzione selezionata. In caso contrario, selezionare **Nome utente** e digitare il nome utente e la password di un account riconosciuto dal server FTP.
5. Selezionare **OK**.

Selezionare **Avanti**.

Passo 4/5 - Scegliere quando eseguire il Backup

Qui potete scegliere quando eseguire il Backup dei vostri dati.


Scegli quando eseguire il backup
Scegli quando eseguire il backup
Fase 4/5
Scegli quando desideri eseguire la procedura di backup
Only backup the data this time
Backup the data on a schedule I specify
< Back
Next >
Cancel

Scegli quando eseguire il backup

Sono disponibili le seguenti opzioni:

- **Eseguire il Backup dei dati solo questa volta**
- **Eseguire il Backup dei dati con una programmazione da me specificata**

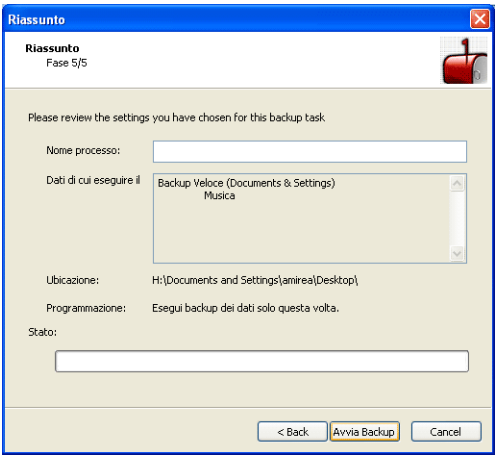
Per eseguire subito il Backup dei dati, cliccare su **Eseguire il Backup dei dati solo questa volta**, per programmare il prodotto in modo da eseguire il Backup dei vostri file in un secondo momento, cliccare su **Eseguire il Backup dei dati con una programmazione da me specificata**.

Se selezionate **Eseguire il backup dei dati con una programmazione da me specificata**, potrete specificare la frequenza con cui la funzione programmata verrà eseguita: giornalmente o settimanalmente. Potrete anche specificare la data e l'ora di inizio.

Selezionare **Avanti**.

Passo 5/5 - Sommario

Qui è possibile rivedere il processo di backup delle impostazioni e avviare il backup.



Riassunto

Dovete inserire un nome della funzione nel campo corrispondente. È possibile effettuare tutte le modifiche con il ritorno a passaggi precedenti (clicca **Torna**).

Cliccare su **Avviare backup** se siete soddisfatti delle vostre impostazioni. Attendere che BitDefender completi il backup e quindi fare clic su **Fine** .

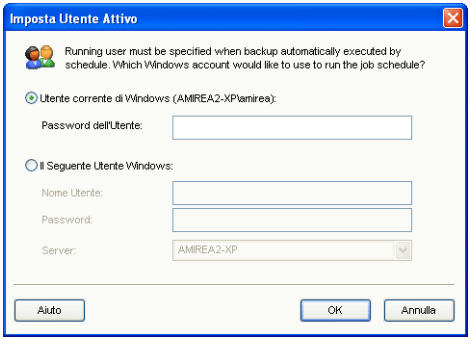
Nota

La prima volta che si crea un processo di backup pianificato, vi verrà chiesto di specificare l'account di Windows utilizzato per eseguire il lavoro.

Per utilizzare l'account utente corrente, è sufficiente digitare la sua password nel campo corrispondente. Se si desidera eseguire il backup con un altro account, seleziona **Il seguente utente di Windows** e compila i campi.

- **Nome utente** - inserire il nome utente dell'account di windows.
- **Password** - inserire la password valida per l'utenza, già specificata precedentemente.
- **Server** - inserisci il nome del dominio server.

Selezionare **OK** per continuare.



Set Running User

11.4.2. Assistente Recupero Locale

Questo assistente aiuta a ripristinare i dati di cui si è effettuato il backup su un dispositivo di archiviazione locale.

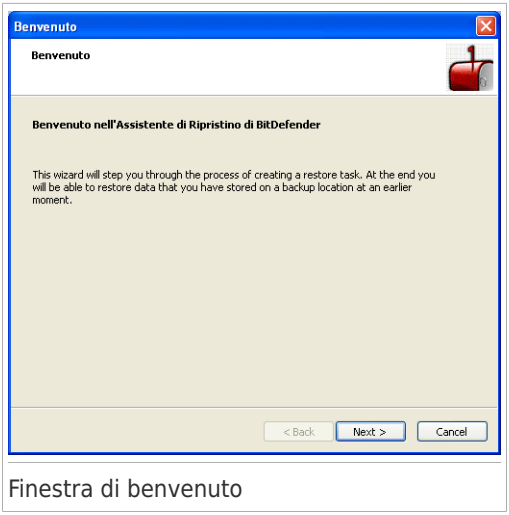
Nota

Prima di ripristinare tutti i dati, assicurarsi che il dispositivo su cui fai il backup sia disponibile. A seconda del dispositivo è stato utilizzato, potrebbe essere necessario prendere una di queste azioni:

- Inserire il backup della chiavetta USB in una porta USB.
- Inserire il backup CD in un drive CD.
- Verificare se è possibile connettersi alla rete o server FTP dove il backup viene memorizzata.

Passo 1/4 - Finestra di Benvenuto

Questa è solo una pagina di benvenuto.

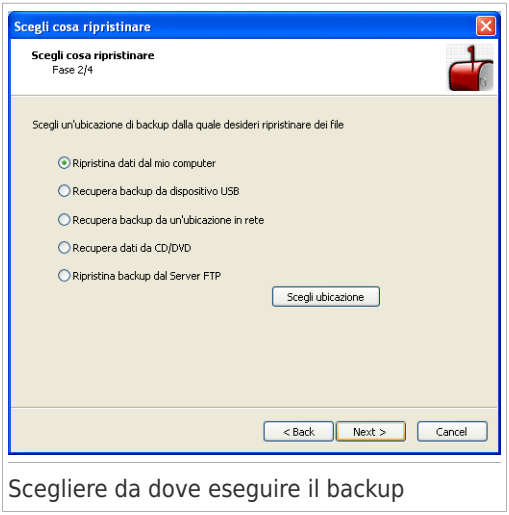

Benvenuto
Benvenuto
Benvenuto nell'Assistente di Ripristino di BitDefender
This wizard will step you through the process of creating a restore task. At the end you will be able to restore data that you have stored on a backup location at an earlier moment.
< Back
Next >
Cancel

Finestra di benvenuto

Selezionare **Avanti**.

Passo 2/4 -Scegliere da dove eseguire il Backup.

Qui potete scegliere l'ubicazione da dove volete ripristinare i file.


Scegli cosa ripristinare
Scegli cosa ripristinare
Fase 2/4
Scegli un'ubicazione di backup dalla quale desideri ripristinare dei file
Ripristina dati dal mio computer
Recupera backup da dispositivo USB
Recupera backup da un'ubicazione in rete
Recupera dati da CD/DVD
Ripristina backup dal Server FTP
Scegli ubicazione
< Back
Next >
Cancel

Scegliere da dove eseguire il backup

Sono disponibili le seguenti opzioni:

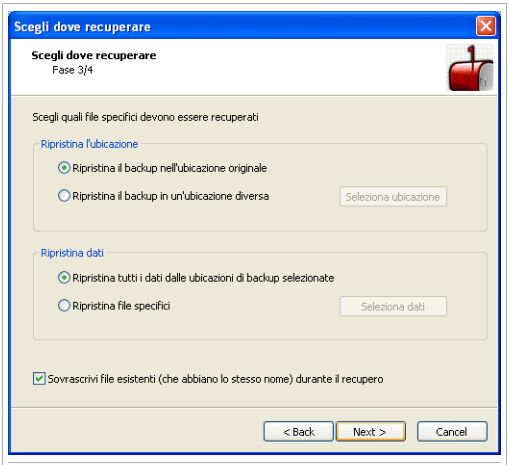
- **Ripristinare i dati dal mio computer**
- **Ripristinare dati da un dispositivo USB**
- **Ripristinare dati da un'ubicazione di rete**
- **Ripristinare dati da un CD/DVD**
- **Ripristinare dati da server FTP**

Dopo aver selezionato l'opzione, fare clic su **Scegli la località** e selezionare il file di backup che si desidera ripristinare.

Selezionare **Avanti**.

Passo 3/4 - Scegliere Ubicazione di Ripristino ed i File

Qui potete scegliere quali specifici file ripristinare e dove ripristinarli.


Scegli dove recuperare
Scegli dove recuperare
Fase 3/4
Scegli quali file specifici devono essere recuperati
Ripristina l'ubicazione
Ripristina il backup nell'ubicazione originale
Ripristina il backup in un'ubicazione diversa
Seleziona ubicazione
Ripristina dati
Ripristina tutti i dati dalle ubicazioni di backup selezionate
Ripristina file specifici
Seleziona dati
Sovrascrivi file esistenti (che abbiano lo stesso nome) durante il recupero
< Back
Next >
Cancel

Scegliere l'ubicazione di ripristino ed i file

Sono disponibili le seguenti opzioni:

- **Ripristinare il backup nell'ubicazione originale**
- **Ripristinare il backup in un'ubicazione diversa**
- **Ripristinare tutti i dati dall'ubicazione di backup selezionata**
- **Ripristinare file specifici**
- **Sostituire file esistenti durante il ripristino**

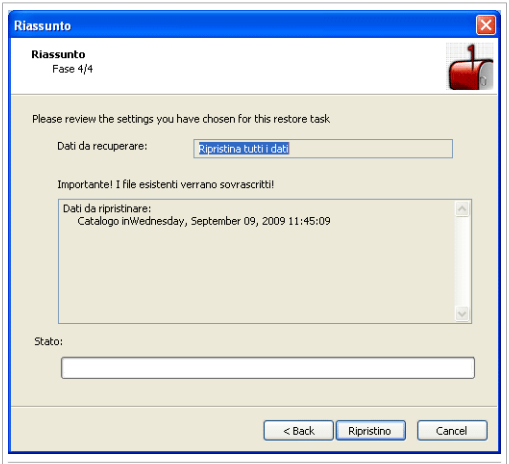
Se si vuole ripristinare dei dati in un'ubicazione diversa o solo file specifici, selezionare l'ubicazione e i dati facendo clic sul pulsante corrispondente.

Onde evitare di sovrascrivere un file esistente durante il ripristino, deselezionare la casella**Sostituire file esistenti durante il ripristino**.

Selezionare **Avanti**.

Passo 4/4 - Sommario

Qui potete rivedere le impostazioni e iniziare il lavoro di ripristino.



Riassunto

Cliccare su **Ripristinare** se siete soddisfatti con le vostre impostazioni. Attendere BitDefender per ripristinare i dati selezionati e quindi fare clic su **Fine** .

11.5. Assistenti di Ottimizzazione

Gli assistenti di Ottimizzazione permettono di ottimizzare lo spazio su disco e migliorare le prestazioni e la reattività del computer.

11.5.1. Procedura guidata Deframmentazione Disco

Questo assistente riorganizza fisicamente i dati sul disco rigido in modo che i frammenti di ogni file siano conservati insieme e in modo continuo.

Nota
La deframmentazione può impiegare un po' di tempo dal momento in cui implica lo spostamento di porzioni di dati immagazzinati da un posto all'altro del disco rigido. Vi consigliamo di eseguire la deframmentazione quando non state usando il vostro computer.

Passo 1/3 - Analisi...

Il Deframmentatore analizzerà il disco rigido per determinare se necessita di essere deframmentato o meno.

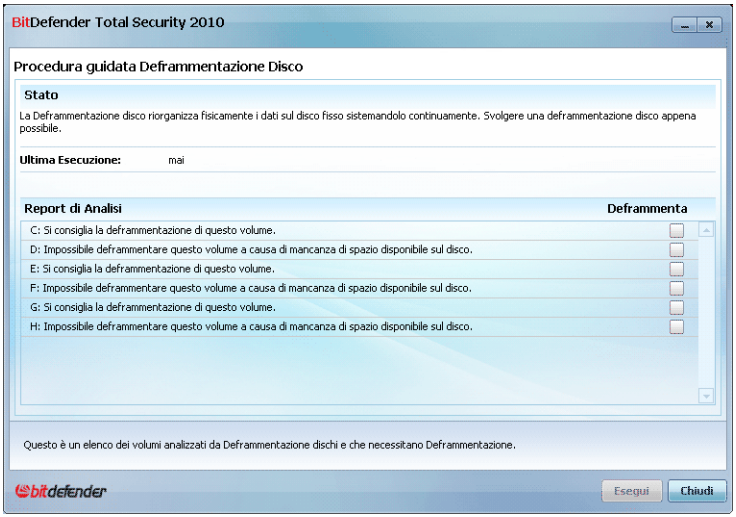
BitDefender Total Security 2010
Procedura guidata Deframmentazione Disco
Analisi in corso
Attendere mentre BitDefender analizza il disco o dischi rigidi per identificare lo stato di deframmentazione per ogni partizione.
Attendere...
Analisi in corso C:
La Deframmentazione dischi sta analizzando il PC in questo momento per determinare i volumi che dovrebbero essere deframmentati.
bitdefender
Annulla

Analisi in corso

Attendere che il Deframmentatore finisca l'analisi. Se desiderate cancellare la operazione, cliccare semplicemente su **Annulla**.

Passo 2/3 - Visualizzare Report di Analisi

Dopo che l'analisi è stata completata, apparirà una nuova finestra dove potrete vedere i risultati ed iniziare la deframmentazione del disco, se necessaria.


BitDefender Total Security 2010
Procedura guidata Deframmentazione Disco
Stato
La Deframmentazione disco riorganizza fisicamente i dati sul disco fisso sistemandolo continuamente. Svolgere una deframmentazione disco appena possibile.
Ultima Esecuzione: mai
Report di Analisi
Deframmenta
C: Si consiglia la deframmentazione di questo volume.
D: Impossibile deframmentare questo volume a causa di mancanza di spazio disponibile sul disco.
E: Si consiglia la deframmentazione di questo volume.
F: Impossibile deframmentare questo volume a causa di mancanza di spazio disponibile sul disco.
G: Si consiglia la deframmentazione di questo volume.
H: Impossibile deframmentare questo volume a causa di mancanza di spazio disponibile sul disco.
Questo è un elenco dei volumi analizzati da Deframmentazione dischi e che necessitano Deframmentazione.
bitdefender
Esegui
Chiudi

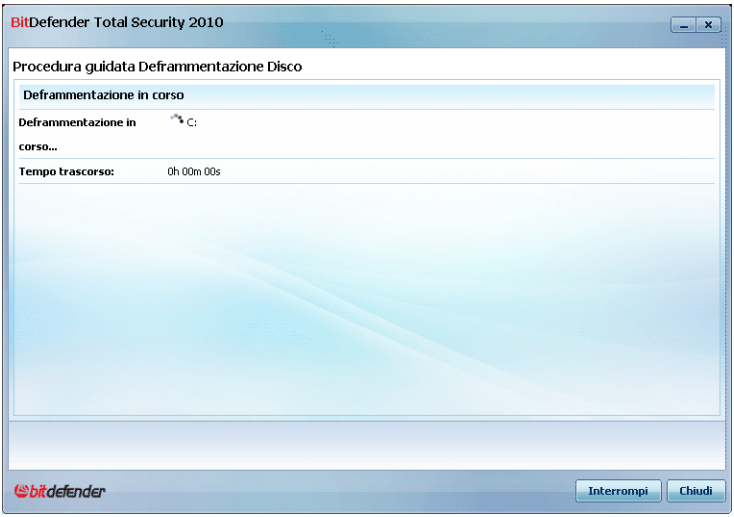
Report di Analisi

Controllare il Report di Analisi

Se nessun disco necessita di deframmentazione, cliccare su **Chiudere** per chiudere la finestra. Altrimenti, selezionare l'opzione **Deframmenta**corrispondente ai volumi che necessitano la deframmentazione e fare clic su **Esegui** per avviare la deframmentazione.

Nota

Il Deframmentatore avrà bisogno del 15% di spazio libero nel volume deframmentato per operare correttamente. Se non c'è spazio libero sufficiente nel volume deframmentato, la deframmentazione verrà interrotta.

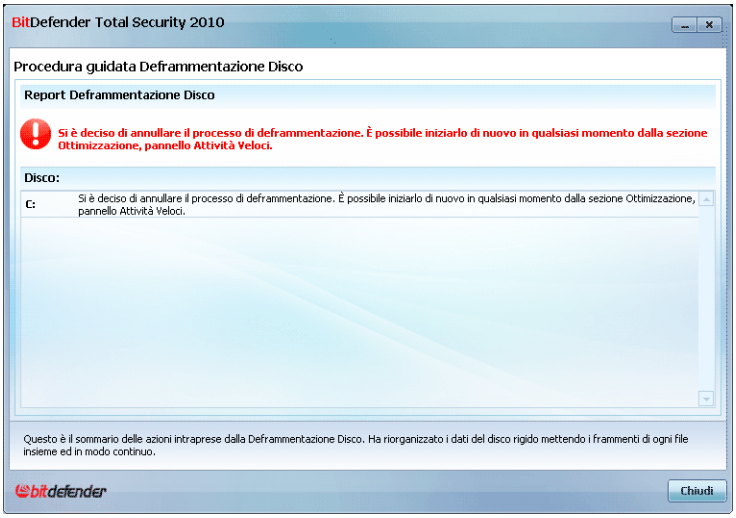


Deframmentando...

Attendere il completamento della deframmentazione del disco. Potete cancellare la deframmentazione del disco in qualsiasi momento cliccando su **Interrompere**.

Passo 3/3 - Visualizzare Report della Deframmentazione

Dopo che la deframmentazione del disco è stata completata, apparirà una nuova finestra dove potrete vedere le statistiche della deframmentazione.


BitDefender Total Security 2010
Procedura guidata Deframmentazione Disco
Report Deframmentazione Disco
Si è deciso di annullare il processo di deframmentazione. È possibile iniziarlo di nuovo in qualsiasi momento dalla sezione Ottimizzazione, pannello Attività Veloci.
Disco:
C:
Si è deciso di annullare il processo di deframmentazione. È possibile iniziarlo di nuovo in qualsiasi momento dalla sezione Ottimizzazione, pannello Attività Veloci.
Questo è il sommario delle azioni intraprese dalla Deframmentazione Disco. Ha riorganizzato i dati del disco rigido mettendo i frammenti di ogni file insieme ed in modo continuo.
bitdefender
Chiudi

Report della Deframmentazione

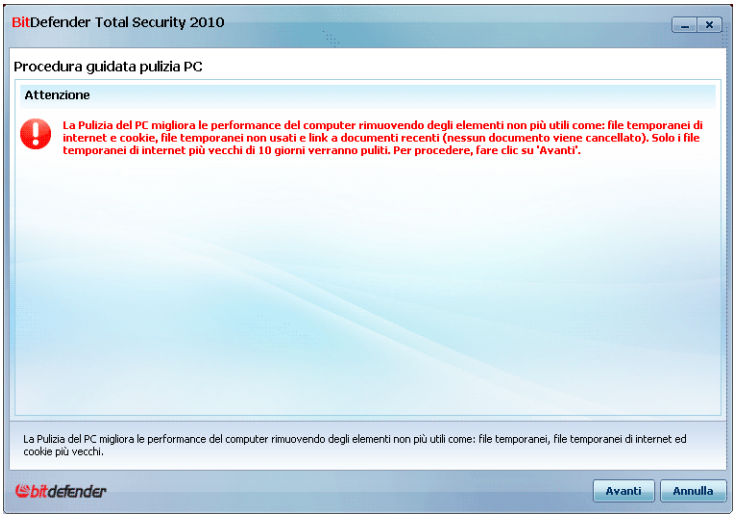
Cliccare su **Chiudere** per chiudere la finestra.

11.5.2. Procedura guidata pulizia PC

Questo assistente rimuove i file non necessari dal disco, inclusi i file temporanei di Internet e i cookie, i file di sistema e i collegamenti ai documenti recenti.

Passo 1/3 – Iniziare Eliminazione

Qui potete inziziare ad eliminare i file temporanei Internet ed i cookies.

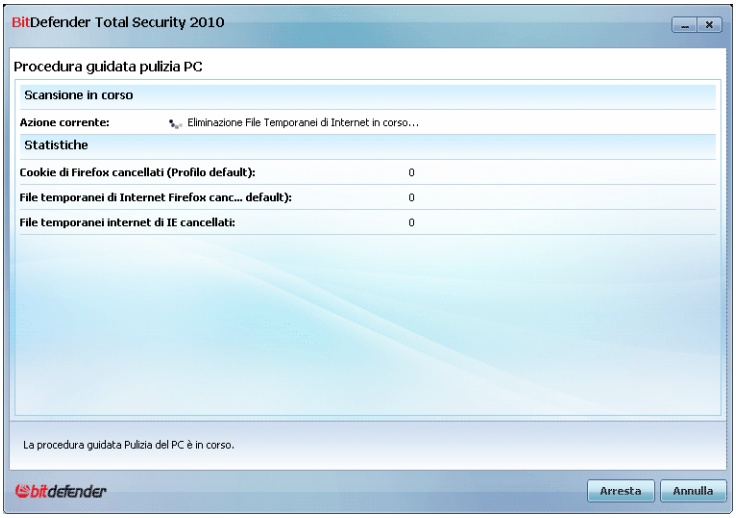

BitDefender Total Security 2010
Procedura guidata pulizia PC
Attenzione
La Pulizia del PC migliora le performance del computer rimuovendo degli elementi non più utili come: file temporanei di internet e cookie, file temporanei non usati e link a documenti recenti (nessun documento viene cancellato). Solo i file temporanei di internet più vecchi di 10 giorni verranno puliti. Per procedere, fare clic su 'Avanti'.
La Pulizia del PC migliora le performance del computer rimuovendo degli elementi non più utili come: file temporanei, file temporanei di internet ed cookie più vecchi.
bitdefender
Avanti
Annulla

Finestra di benvenuto

Selezionare **Avanti**.

Passo 1/3 – Eliminando file...

Lo strumento di pulizia inizierà ad eliminare i file temporanei Internet ed i cookies.

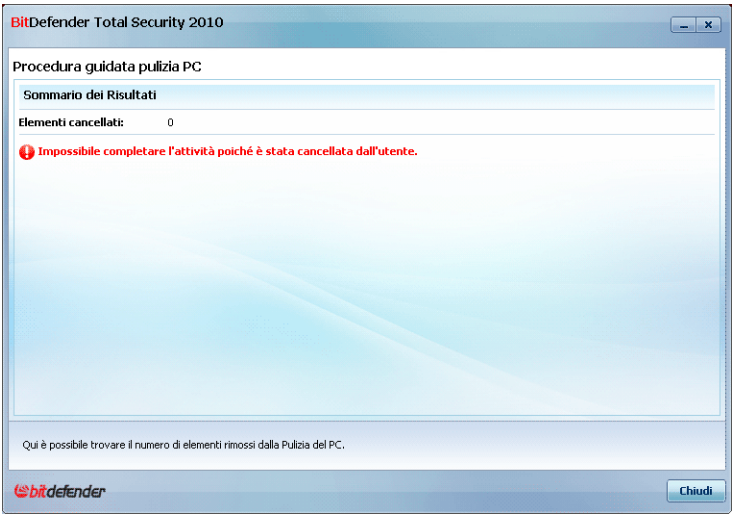


Eliminando File...

Attendere che lo strumento di pulizia elimini i file temporanei Internet ed i cookies. Se desiderate cancellare la operazione, cliccare semplicemente su **Annulla**.

Passo 3/3 - Visualizzare Sommario dei Risultati

Dopo che lo strumento di pulizia ha eliminato tutti i file, apparirà una nuova finestra nella quale potrete vedere il sommario dei risultati.


BitDefender Total Security 2010
Procedura guidata pulizia PC
Sommario dei Risultati
Elementi cancellati: 0
Impossibile completare l'attività poiché è stata cancellata dall'utente.
Qui è possibile trovare il numero di elementi rimossi dalla Pulizia del PC.
bitdefender
Chiudi

Sommario dei Risultati

Potete vedere le statistiche riguardanti gli oggetti eliminati.

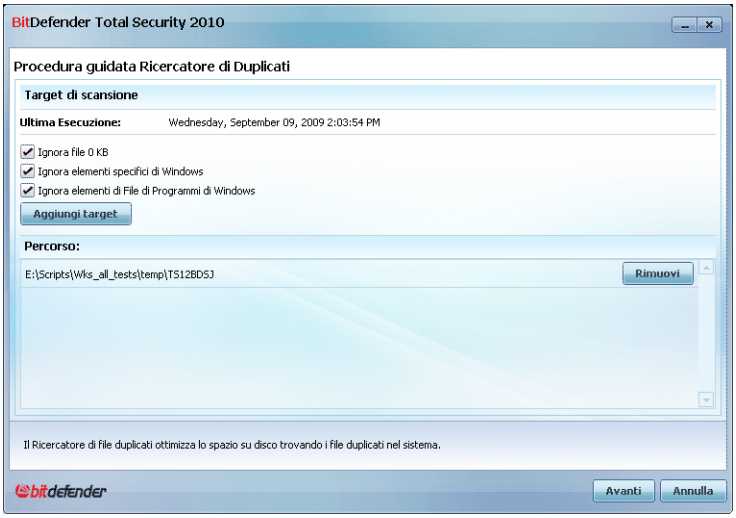
Cliccare su **Chiudere** per chiudere la finestra.

11.5.3. Procedura guidata Ricercatore di Duplicati

Questo assistente permette di trovare e cancellare i file duplicati sul sistema.

Passo 1/4 – Selezione del Target di ricerca

Qui potete specificare dove cercare i duplicati.



Target di ricerca

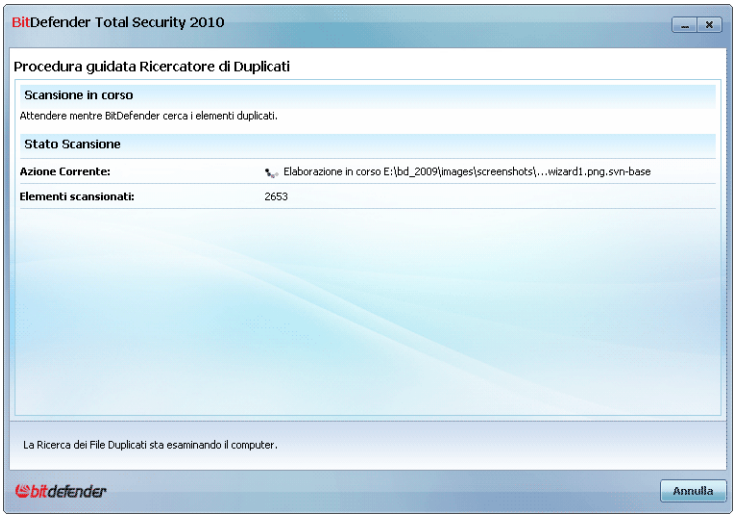
Cliccare su **Aggiungi Target** e selezionare l'ubicazione dove il Ricercatore di Duplicati(ricerca di duplicati) deve cercare i file duplicati. Il percorso all'ubicazione selezionata apparirà nella colonna **Percorso**. Se si cambia idea circa la locazione, sarà sufficiente fare clic sul pulsante **Rimuovere** vicino.

Nota
E' possibile selezionare una o più ubicazioni.

Selezionare **Avanti**.

Passo 2/4 – Ricerca...

Il Ricercatore di Duplicati inizierà a cercare i file duplicati.



Cercando...

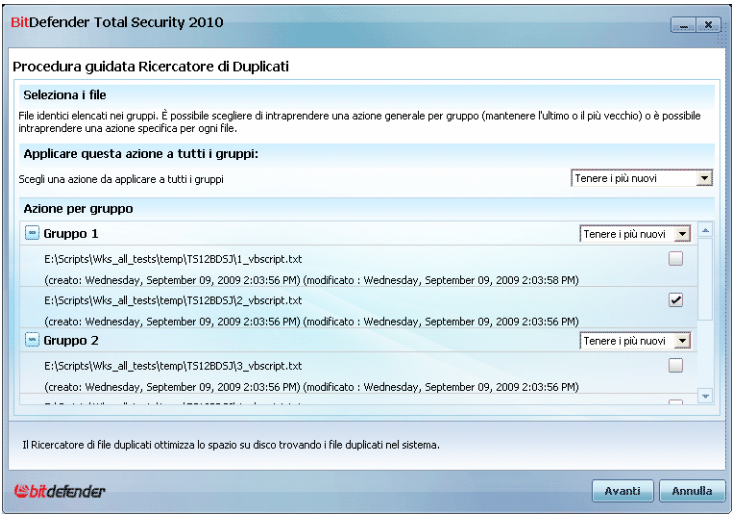
Potete veder lo stato e le statistiche della ricerca.

Attendere che il Ricercatore di Duplicati finisca la ricerca di file duplicati. Se desiderate cancellare la operazione, cliccare semplicemente su **Annulla**.

Passo 3/4 – Selezionare azione

Dopo che la ricerca è stata completata, apparirà una nuova finestra dove potrete specificare quali azioni intraprendere sui file duplicati rilevati.

Nota
Se nessun file duplicato è stato trovato, ignorerete questo passo.


BitDefender Total Security 2010
Procedura guidata Ricercatore di Duplicati
Seleziona i file
File identici elencati nei gruppi. È possibile scegliere di intraprendere una azione generale per gruppo (mantenere l'ultimo o il più vecchio) o è possibile intraprendere una azione specifica per ogni file.
Applicare questa azione a tutti i gruppi:
Scegli una azione da applicare a tutti i gruppi
Tenere i più nuovi
Azione per gruppo
Gruppo 1
Tenere i più nuovi
E:\Scripts\Wks_all_tests\temp\TS12BDSJ\1_vbscript.txt
(creato: Wednesday, September 09, 2009 2:03:56 PM) (modificato : Wednesday, September 09, 2009 2:03:58 PM)
E:\Scripts\Wks_all_tests\temp\TS12BDSJ\2_vbscript.txt
(creato: Wednesday, September 09, 2009 2:03:56 PM) (modificato : Wednesday, September 09, 2009 2:03:56 PM)
Gruppo 2
Tenere i più nuovi
E:\Scripts\Wks_all_tests\temp\TS12BDSJ\3_vbscript.txt
(creato: Wednesday, September 09, 2009 2:03:56 PM) (modificato : Wednesday, September 09, 2009 2:03:56 PM)
Il Ricercatore di file duplicati ottimizza lo spazio su disco trovando i file duplicati nel sistema.
bitdefender
Avanti
Annulla

Azioni

I file duplicati rilevati vengono organizzati e mostrati in gruppi. Se cliccate vicino ad un gruppo, potrete visualizzare le informazioni dettagliate sui file duplicati (percorso completo, dimensione, data di creazione e di modifica).

Potete scegliere un'azione complessiva da eseguire su tutti i file duplicati rilevati oppure potete scegliere delle azioni da eseguire su gruppi di file duplicati. Le seguenti azioni sono disponibili nel menu:

Azione	Descrizione
Mantenere il più recente	Il duplicato più recente verrà conservato, mentre gli altri verranno eliminati.
Mantenere il più vecchio	Il duplicato più vecchio verrà conservato, mentre gli altri verranno eliminati.
Nessuna azione	Nessuna azione verrà eseguita sui file duplicati.

Se volete applicare un'azione complessiva a tutti gli oggetti di un gruppo, selezionare l'azione desiderata dal menu corrispondente. Se volete che vengano eliminati solo dei file specifici del gruppo, selezionate l'opzione **Eliminare** accanto ai rispettivi file.

Nota

L'azione complessiva non sovrascriverà l'azione scelta per file specifici o gruppi. Questo significa che, se impostate, per esempio, **Mantenere il più recente** come azione complessiva ma scegliete di non eseguire alcuna azione su di un gruppo in particolare, allora l'azione complessiva verrà applicata a tutti i gruppi, tranne che a quel gruppo particolare.

Selezionare **Avanti**.

Passo 4/4 - Visualizzare Sommario dei Risultati

Qui potete visualizzare i risultati della scansione del Ricercatore di Duplicati.

BitDefender Total Security 2010
Procedura guidata Ricercatore di Duplicati
Sommario dei Risultati
Tutti i file contrassegnati per l'eliminazione sono stati eliminati.
Elementi scansionati: 6
Gruppi di file duplicati: 3
File duplicati: 6
Questo è il sommario delle azioni intraprese dal Ricercatore Duplicati, incluso il numero di problemi trovati e gli elementi scansionati, il numero di gruppi di file duplicati (un insieme di file che includono tutti gli stessi dati) e il numero di file duplicati rilevati.
bitdefender
Chiudi

Sommario dei Risultati

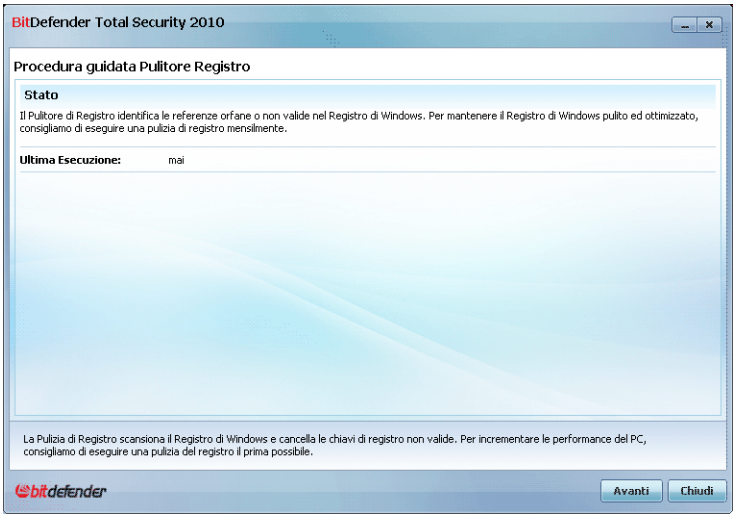
Cliccare su **Eseguire nuovamente** per iniziare una nuova ricerca di file duplicati o su **OK** per chiudere la finestra.

11.5.4. Procedura guidata Pulitore Registro

Questo assistente identifica e cancella i riferimenti non validi od orfani del Registro di Sistema di Windows.

Passo 1/4 - Iniziare scansione

Qui potete avviare la scansione del registro.


BitDefender Total Security 2010
Procedura guidata Pulitore Registro
Stato
Il Pulitore di Registro identifica le referenze orfane o non valide nel Registro di Windows. Per mantenere il Registro di Windows pulito ed ottimizzato, consigliamo di eseguire una pulizia di registro mensilmente.
Ultima Esecuzione: mai
La Pulizia di Registro scansiona il Registro di Windows e cancella le chiavi di registro non valide. Per incrementare le performance del PC, consigliamo di eseguire una pulizia del registro il prima possibile.
bitdefender
Avanti
Chiudi

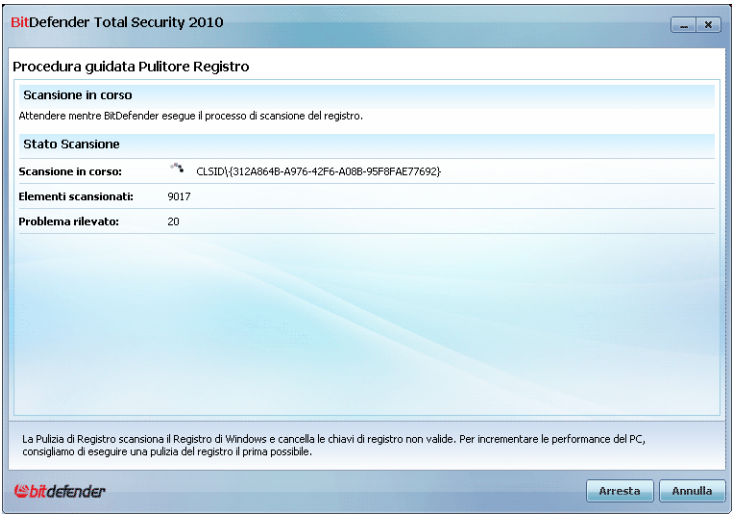
Stato

Potete vedere quando è stata eseguita per l'ultima volta la Pulizia del Registro e la raccomandazione di BitDefender.

Selezionare **Avanti**.

Passo 2/4 - Esaminando...

Lo Strumento di Pulizia di Registro avvierà la scansione del Registro di Windows.


BitDefender Total Security 2010
Procedura guidata Pulitore Registro
Scansione in corso
Attendere mentre BitDefender esegue il processo di scansione del registro.
Stato Scansione
Scansione in corso:
CLSID\{312A864B-A976-42F6-A08B-95F8FAE77692}
Elementi scansionati:
9017
Problema rilevato:
20
La Pulizia di Registro scansiona il Registro di Windows e cancella le chiavi di registro non valide. Per incrementare le performance del PC, consigliamo di eseguire una pulizia del registro il prima possibile.
bitdefender
Arresta
Annulla

Scansione in corso...

Potete vedere l'ultima chiave di registro esaminata e le relative statistiche.

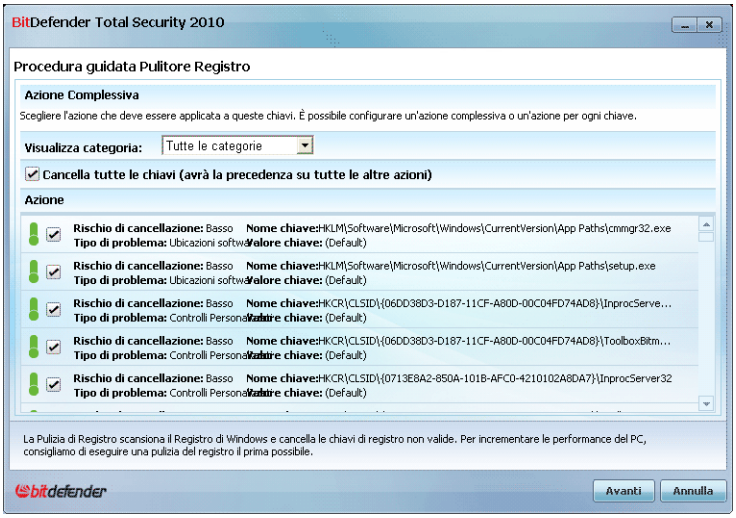
Attendere che lo Strumento di Pulizia di Registro completi la scansione della chiave di registro. Se desiderate cancellare la operazione, cliccare semplicemente su **Annulla**.

Nota
Se volete fermare la scansione, cliccate semplicemente **Fermare**. Ignorerete il passo seguente.

Passo 3/4 – Selezionare azione

Una volta completata la scansione delle chiavi di registro, apparirà una nuova finestra dove potrete vedere i risultati.

Nota
Se non viene riscontrato alcun problema o se avete scelto di fermare la scansione, ignorerete questo passo.


BitDefender Total Security 2010
Procedura guidata Pulitore Registro
Azione Complessiva
Scegliere l'azione che deve essere applicata a queste chiavi. È possibile configurare un'azione complessiva o un'azione per ogni chiave.
Visualizza categoria:
Tutte le categorie
Cancella tutte le chiavi (avrà la precedenza su tutte le altre azioni)
Azione
Rischio di cancellazione: Basso
Nome chiave:HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths\cmmgr32.exe
Tipo di problema: Ubicazioni softwa
Valore chiave: (Default)
Rischio di cancellazione: Basso
Nome chiave:HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths\setup.exe
Tipo di problema: Ubicazioni softwa
Valore chiave: (Default)
Rischio di cancellazione: Basso
Nome chiave:HKCR\CLSID\{06DD38D3-D187-11CF-A80D-00C04FD74AD8}\InprocServe...
Tipo di problema: Controlli Personal
Valore chiave: (Default)
Rischio di cancellazione: Basso
Nome chiave:HKCR\CLSID\{06DD38D3-D187-11CF-A80D-00C04FD74AD8}\ToolboxBitm...
Tipo di problema: Controlli Personal
Valore chiave: (Default)
Rischio di cancellazione: Basso
Nome chiave:HKCR\CLSID\{0713E8A2-850A-101B-AFC0-4210102A8DA7}\InprocServer32
Tipo di problema: Controlli Personal
Valore chiave: (Default)
La Pulizia di Registro scansiona il Registro di Windows e cancella le chiavi di registro non valide. Per incrementare le performance del PC, consigliamo di eseguire una pulizia del registro il prima possibile.
bitdefender
Avanti
Annulla

Azioni

Potete visualizzare tutte le chiavi di registro orfane o non valide rilevate. Vengono fornite informazioni dettagliate su ogni chiave di registro (nome, valore, priorità, categoria)

Le chiavi di registro vengono raggruppate in base alla loro posizione nel Registro di Windows.

Categoria	Descrizione
Ubicazioni Software	Le chiavi di registro che contengono informazioni sul percorso di applicazioni installate sul vostro computer. Alle chiavi non valide viene assegnata una priorità bassa, in modo che possiate cancellarle senza praticamente nessun rischio.
Controlli Personalizzati	Chiavi di registro che contengono informazioni sulle estensioni dei file registrate sul vostro computer. Queste chiavi di registro vengono comunemente usate per mantenere le associazioni dei file (per assicurare che si apre il programma giusto quando aprite un file usando Windows Explorer). Ad esempio, una chiave di registro di questo tipo permette a Windows di aprire un file `.doc` con Microsoft Word.

Categoria	Descrizione
	Alle chiavi non valide viene assegnata una priorità bassa, in modo che possiate cancellarle senza praticamente nessun rischio.
DLL condivise	Chiavi di registro che contengono informazioni sulla posizione delle DLL (Dynamic Link Libraries) condivise. Le DLL immagazzinano funzioni che vengono usate dalle applicazioni installate per eseguire certi task. Possono essere condivise da diverse applicazioni per ridurre i requisiti di memoria e di spazio su disco. Queste chiavi di registro diventano invalide quando la DLL sulla quale puntano viene spostata ad un'altra posizione o completamente rimossa (questo occorre normalmente quando disinstallate un programma). Alle chiavi invalide viene assegnata una priorità media, quindi cancellarle potrebbe interessare negativamente il sistema.

Per gestire più facilmente il processo di pulizia, potete selezionare una categoria dal menu.

Potete scegliere di cancellare tutte o solo delle specifiche chiavi non valide dalla categoria selezionata. Se selezionate **Eliminare tutte le chiavi** tutte le chiavi rilevate verranno eliminate. Se desiderate eliminare solo delle chiavi specifiche, selezionate l'opzione **Eliminare** accanto alle rispettive chiavi.

Nota
Di default, tutte le chiavi non valide rilevate verranno eliminate.

Selezionare **Avanti**.

Passo 4/4 - Visualizzare Sommario dei Risultati

Qui potete vedere i risultati della scansione eseguita dallo Strumento di Pulizia di Registro.

BitDefender Total Security 2010
Procedura guidata Pulitore Registro
Sommario dei Risultati
Sotto è possibile vedere i risultati della Pulizia di Registro.
Problema rilevato: 374
Chiavi cancellate: 374
Chiavi ignorate: 0
Questo è il sommario di questo processo di pulizia di registro. Qui è possibile vedere il numero di problemi trovati ed il numero di chiavi cancellate oppure ignorate.
bitdefender
Chiudi

Sommario dei Risultati

Se non avete scelto di eliminare tutte le chiavi di registro, vi verrà mostrato un testo di avviso. Vi consigliamo di rivedere i rispettivi problemi.

Cliccare su **Chiudere** per chiudere la finestra.

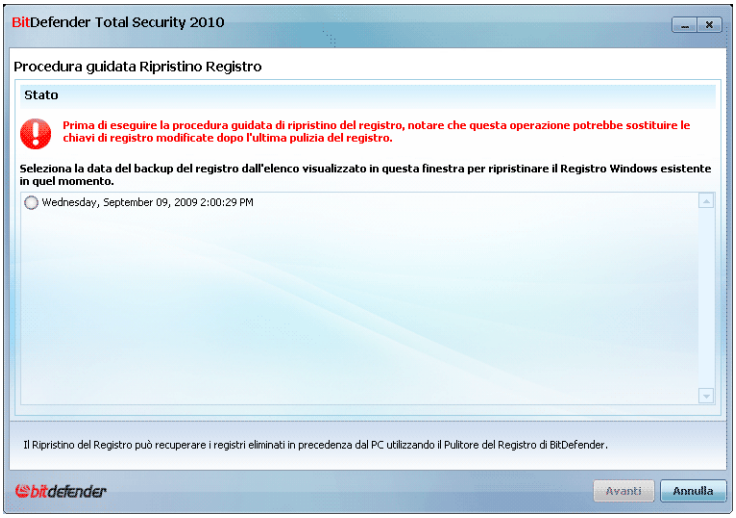
11.5.5. Procedura guidata Ripristino Registro

Questo assistente permette di recuperare le chiavi di registro precedentemente cancellate dal Registro di Sistema di Windows utilizzando la Pulizia del Registro di BitDefender.

Importante
Solo gli utenti con diritti di amministrazione possono recuperare il registro pulito.

Passo 1/2 - Avviare Recupero del Registro

Qui potete avviare il recupero del registro pulito.


BitDefender Total Security 2010
Procedura guidata Ripristino Registro
Stato
Prima di eseguire la procedura guidata di ripristino del registro, notare che questa operazione potrebbe sostituire le chiavi di registro modificate dopo l'ultima pulizia del registro.
Seleziona la data del backup del registro dall'elenco visualizzato in questa finestra per ripristinare il Registro Windows esistente in quel momento.
Wednesday, September 09, 2009 2:00:29 PM
Il Ripristino del Registro può recuperare i registri eliminati in precedenza dal PC utilizzando il Pulitore del Registro di BitDefender.
bitdefender
Avanti
Annulla

Stato

Potete vedere un elenco di momenti in cui il Registro di Windows è stato pulito. Selezionare il momento dal quale ripristinare il Registro di Windows.

Se siete sicuri di voler recuperare le chiavi di registro cancellate nel momento selezionato, cliccare su **Avanti**.

Avvertimento
Il recupero del registro pulito potrebbe sovrascrivere le chiavi di registro modificate dopo l'ultima pulizia.

Passo 2/2 - Visualizzare Risultati

Qui potete vedere se il recupero è stato eseguito con successo.

BitDefender Total Security 2010
Procedura guidata Ripristino Registro
Operazione completata con successo.
Il Ripristino del Registro può recuperare i registri eliminati in precedenza dal PC utilizzando il Pulitore del Registro di BitDefender.
bitdefender
Chiudi

Risultati

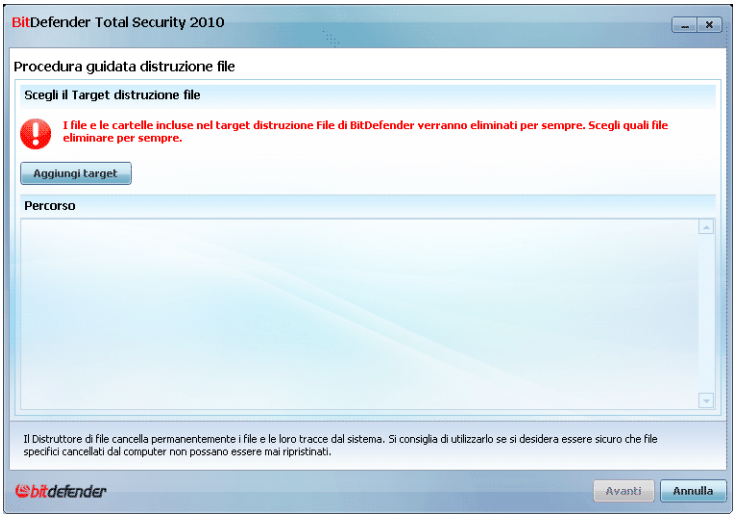
Cliccare su **Chiudere** per chiudere la finestra.

11.5.6. Procedura guidata distruzione file

Questo assistente permette di cancellare permanentemente dal sistema i file ed ogni loro traccia. Utilizzare l'eliminazione definitiva dei file per assicurarvi che i file cancellati dal vostro computer non possano essere mai più recuperati.

Passo 1/3 - Selezionare Target

Qui potete specificare i file o cartelle da rimuovere definitivamente.


BitDefender Total Security 2010
Procedura guidata distruzione file
Scegli il Target distruzione file
I file e le cartelle incluse nel target distruzione File di BitDefender verranno eliminati per sempre. Scegli quali file eliminare per sempre.
Aggiungi target
Percorso
Il Distruttore di file cancella permanentemente i file e le loro tracce dal sistema. Si consiglia di utilizzarlo se si desidera essere sicuro che file specifici cancellati dal computer non possano essere mai ripristinati.
bitdefender
Avanti
Annulla

Target

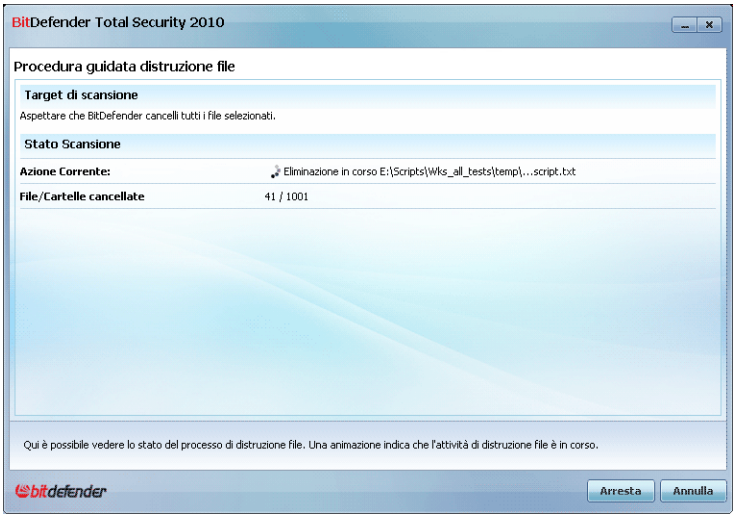
Cliccare su **Aggiungere Target**, selezionare il file o cartella che volete eliminare e cliccare su **OK**. Il percorso all'ubicazione selezionata apparirà nella colonna **Percorso**. Se si cambia idea circa la locazione, sarà sufficiente fare clic sul pulsante **Rimuovere** vicino.

Nota
E' possibile selezionare una o più ubicazioni.

Selezionare **Avanti**.

Passo 1/3 – Eliminando file...

BitDefender eliminerà definitivamente i file nelle ubicazioni specificate.


BitDefender Total Security 2010
Procedura guidata distruzione file
Target di scansione
Aspettare che BitDefender cancelli tutti i file selezionati.
Stato Scansione
Azione Corrente:
Eliminazione in corso E:\Scripts\Wks_all_tests\temp\...script.txt
File/Cartelle cancellate
41 / 1001
Qui è possibile vedere lo stato del processo di distruzione file. Una animazione indica che l'attività di distruzione file è in corso.
bitdefender
Arresta
Annulla

Cancellazione in corso...

Attendere il completamento dell'operazione di eliminazione definitiva del file. Se desiderate cancellare la operazione, cliccare semplicemente su **Annulla**.

Passo 3/3 - Visualizzare Sommario dei Risultati

Dopo che tutti i file saranno stati rimossi, apparirà una nuova finestra dove potrete visualizzare i risultati.

BitDefender Total Security 2010
Procedura guidata distruzione file
Sommario dei Risultati
Tutti i file e cartelle contrassegnati sono stati permanentemente cancellati!
File cancellati definitivamente: 1
Cartelle cancellate definitivamente: 1
File non eliminati: 0
Cartelle non eliminate: 0
Questo è il sommario del processo di distruzione file attuale. Qui è possibile vedere il numero di file e cartelle che sono state eliminate per sempre insieme al numero di file e cartelle che non è stato possibile eliminare.
bitdefender
Chiudi

Sommario dei Risultati

Cliccare su **Chiudere** per chiudere la finestra.

11.6. Assistente File Vault

L'assistente File Vault permette di creare e gestire i file vault di BitDefender. Un file vault è uno spazio di memorizzazione criptato sul computer, dove i file, i documenti e perfino intere cartelle possono essere conservati in sicurezza.

Questi assistenti non appaiono quando vengono risolti i problemi, poiché i file vault sono un metodo opzionale di protezione dei dati. Possono essere avviati solo dall'interfaccia Modalità Intermedia di BitDefender, alla scheda **Archiviazione File**, nel modo seguente:

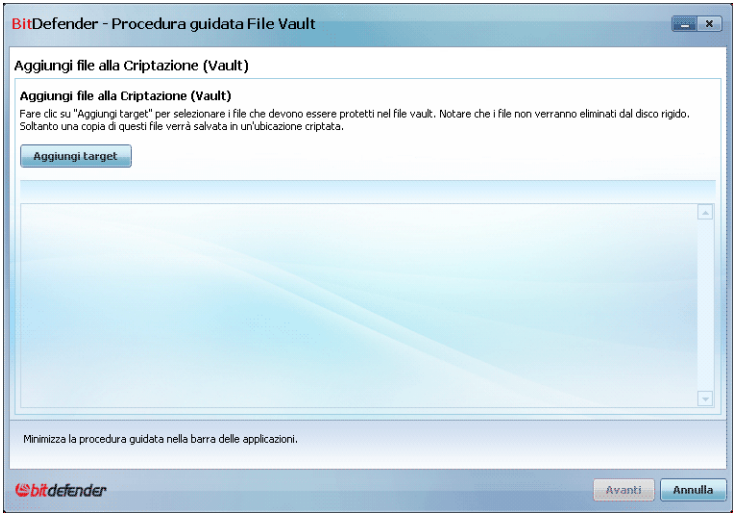
- **Aggiungere File alla Criptazione** - inizia la procedura guidata che vi permette di immagazzinare i vostri file / documenti importanti privatamente mediante la loro criptazione in speciali drive protetti.
- **Rimuovere File dalla Criptazione** - inizia la procedura guidata che vi permette di cancellare dati dai file prottetti.
- **Visualizzare File Vault** - inizia la procedura guidata che vi permette di visualizzare il contenuto dei file vault.
- **Bloccare File Vault** - inizia la procedura guidata che permette di bloccare un file vault aperto per proteggere il suo contenuto.

11.6.1. Aggiungi file alla Criptazione (Vault)

Questo assistente permette di creare un file vault e aggiungere file ad esso per memorizzarli in sicurezza sul computer.

Passo 1/6 - Selezionare Target

Qua potete specificare i file o cartelle da aggiungere al vault.


BitDefender - Procedura guidata File Vault
Aggiungi file alla Criptazione (Vault)
Aggiungi file alla Criptazione (Vault)
Fare clic su "Aggiungi target" per selezionare i file che devono essere protetti nel file vault. Notare che i file non verranno eliminati dal disco rigido. Soltanto una copia di questi file verrà salvata in un'ubicazione criptata.
Aggiungi target
Minimizza la procedura guidata nella barra delle applicazioni.
bitdefender
Avanti
Annulla

Target

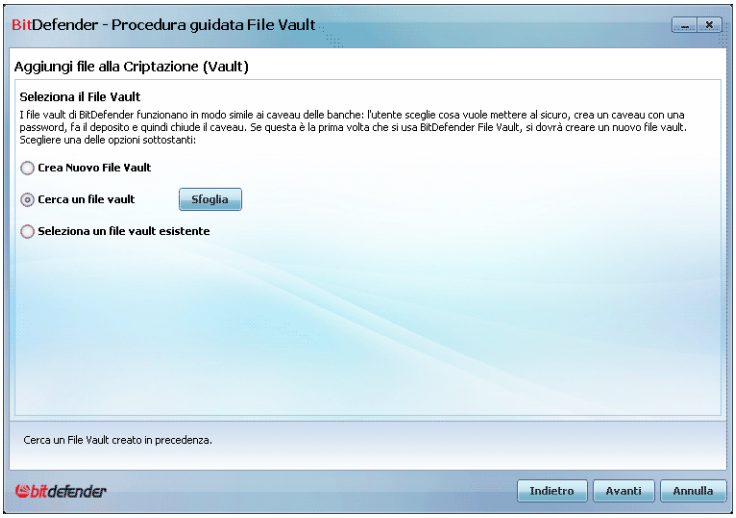
Cliccare su **Aggiungere Target**, selezionare il file o la cartella che si vuole aggiungere e cliccare **OK**. Il percorso all'ubicazione selezionata apparirà nella colonna **Percorso**. Se si cambia idea circa la locazione, sarà sufficiente fare clic sul pulsante **Rimuovere** vicino.

Nota
E' possibile selezionare una o più ubicazioni.

Selezionare **Avanti**.

Passo 2/6 - Selezionare Vault

Qui potete creare un nuovo vault o scegliere uno esistente.


BitDefender - Procedura guidata File Vault
Aggiungi file alla Criptazione (Vault)
Seleziona il File Vault
I file vault di BitDefender funzionano in modo simile ai caveau delle banche: l'utente sceglie cosa vuole mettere al sicuro, crea un caveau con una password, fa il deposito e quindi chiude il caveau. Se questa è la prima volta che si usa BitDefender File Vault, si dovrà creare un nuovo file vault. Scegliere una delle opzioni sottostanti:
Crea Nuovo File Vault
Cerca un file vault
Sfoglia
Seleziona un file vault esistente
Cerca un File Vault creato in precedenza.
bitdefender
Indietro
Avanti
Annulla

Seleziona Vault

Se selezionate **Trovare un Vault File**, dovete cliccare su **Sfoglia** e selezionare il vault. Dovrete andare al passo 5 se il vault selezionato è aperto (montato) o al passo 4 se è bloccato (smontato).

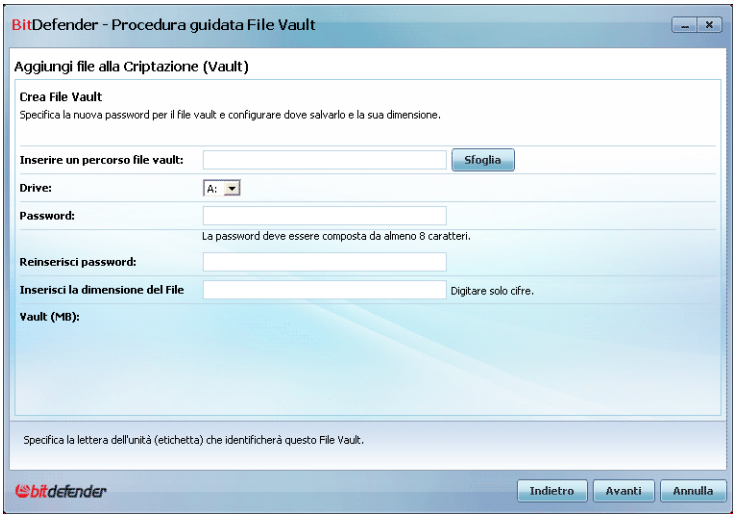
Se cliccate su **Selezionare un Vault esistente**, dovrete poi cliccare sul nome del vault desiderato. Dovrete andare al passo 5 se il vault selezionato è aperto (montato) o al passo 4 se è bloccato (smontato).

Selezionare **Creare Nuovo Vault File** se nessuno di quelli esistenti si adatta alle vostre necessità. Andrete quindi al passo 3.

Selezionare **Avanti**.

Passo 3/6 - Creare Vault

Qui è dove potrete specificare le linformazioni per il nuovo Vault.



Crea Vault

Per completare l'informazione relativa al vault, seguire questi passaggi:

1. Cliccare su **Sfoglia** e scegliere una destinazione per il file bvd.

   Nota
   Ricordare che il vault file è un file criptato sul vostro computer con estensione bvd.

2. Selezionare la lettera del drive per il nuovo file criptato dal corrispondente menu a tendina.

   Nota
   Ricordare che quando montate il file bvd, apparirà una nuova partizione logica (un nuovo drive).

3. Digitare una password per la criptazione del file nel campo corrispondente.

   Nota
   La password deve essere composta da almeno 8 caratteri.

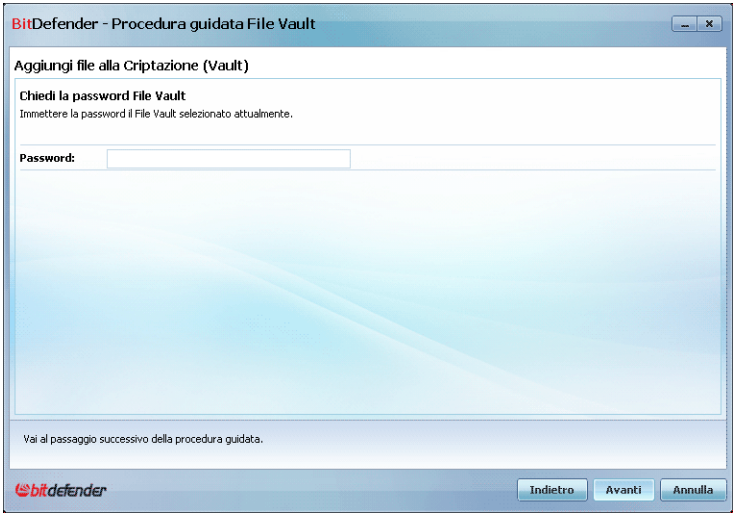
4. Re-inserire la password.
5. Impostare la dimensione del vault (in MB) digitando un numero nel campo corrispondente.

Selezionare **Avanti**.

Andrete al passo 5.

Passo 4/6 – Password

Qui è dove vi verrà chiesto di inserire la password per il vault selezionato.

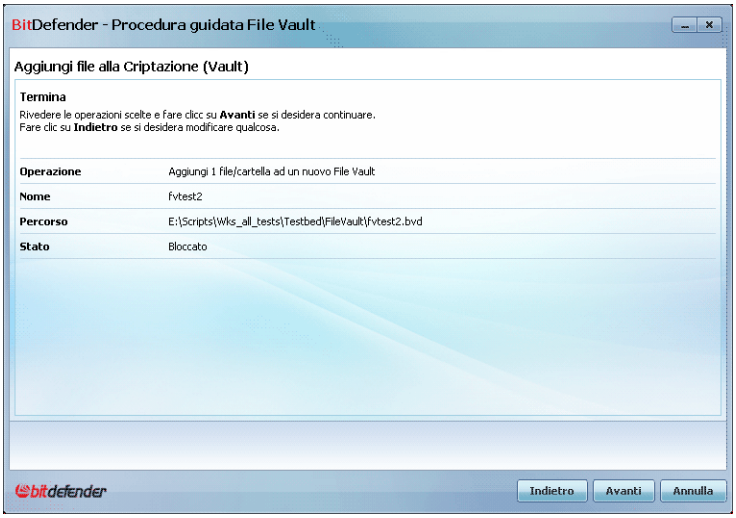


Conferma password

Digitare la password nel campo corrispondente e cliccare su **Avanti**.

Passo 5/6 – Sommario

Qui è dove potrete rivedere le operazioni selezionate.

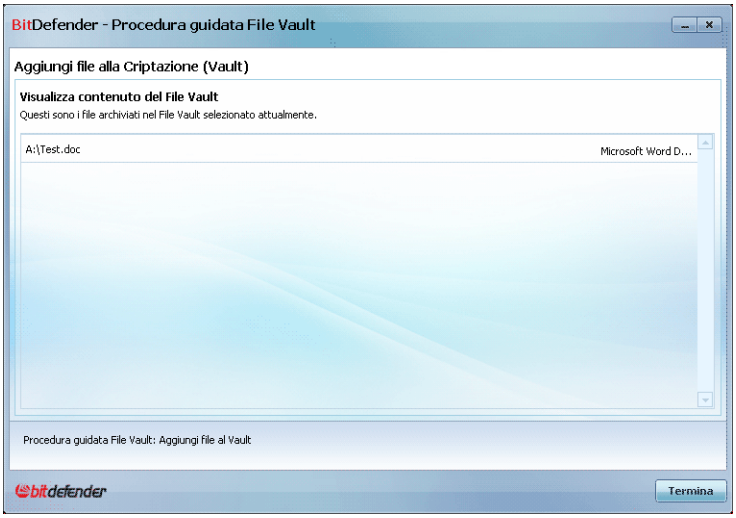


Riassunto

Selezionare **Avanti**.

Passo 6/6 – Risultati

Qui è dove potete vedere il contenuto del vault.


BitDefender - Procedura guidata File Vault
Aggiungi file alla Criptazione (Vault)
Visualizza contenuto del File Vault
Questi sono i file archiviati nel File Vault selezionato attualmente.
A:\Test.doc
Microsoft Word D...
Procedura guidata File Vault: Aggiungi file al Vault
bitdefender
Termina

Risultati

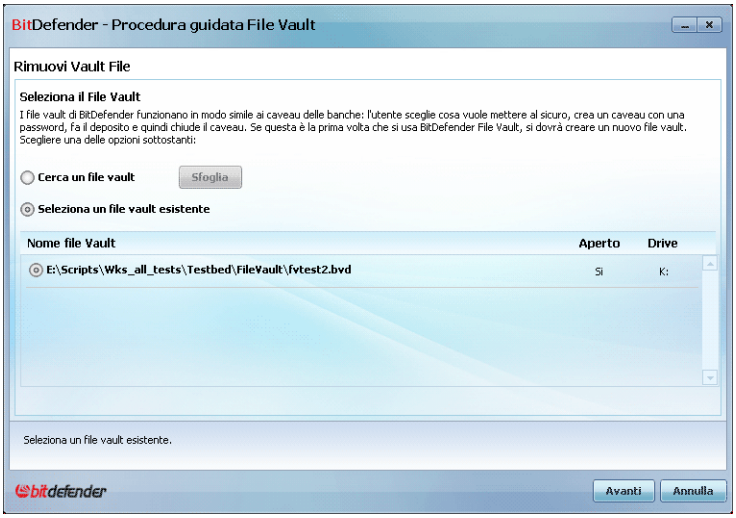
Selezionare **Termina**.

11.6.2. Rimuovi Vault File

Questo assistente permette di rimuovere file da uno specifico file vault.

Passo 1/5 - Selezionare Vault

Qui potete specificare il vault dal quale rimuovere i file.


BitDefender - Procedura guidata File Vault
Rimuovi Vault File
Seleziona il File Vault
I file vault di BitDefender funzionano in modo simile ai caveau delle banche: l'utente sceglie cosa vuole mettere al sicuro, crea un caveau con una password, fa il deposito e quindi chiude il caveau. Se questa è la prima volta che si usa BitDefender File Vault, si dovrà creare un nuovo file vault. Scegliere una delle opzioni sottostanti:
Cerca un file vault
Sfoglia
Seleziona un file vault esistente
Nome file Vault
Aperto
Drive
E:\Scripts\Wks_all_tests\Testbed\FileVault\fvtest2.bvd
Si
K:
Seleziona un file vault esistente.
bitdefender
Avanti
Annulla

Seleziona Vault

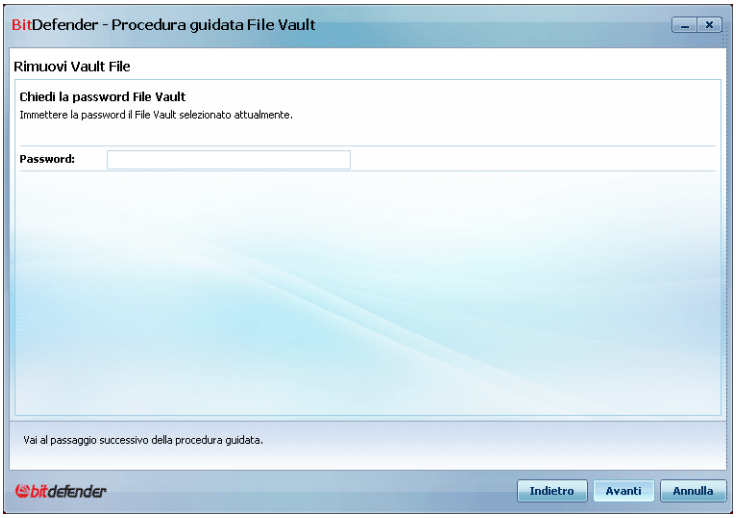
Se selezionate **Trovare un Vault File**, dovete cliccare su **Sfoglia** e selezionare il vault. Dovrete andare al passo 3 se il vault selezionato è aperto (montato) o al passo 2 se è bloccato (smontato).

Se cliccate su **Selezionare un Vault esistente**, dovrete poi cliccare sul nome del vault desiderato. Dovrete andare al passo 3 se il vault selezionato è aperto (montato) o al passo 2 se è bloccato (smontato).

Selezionare **Avanti**.

Passo 2/5 - Password

Qui è dove vi verrà chiesto di inserire la password per il vault selezionato.

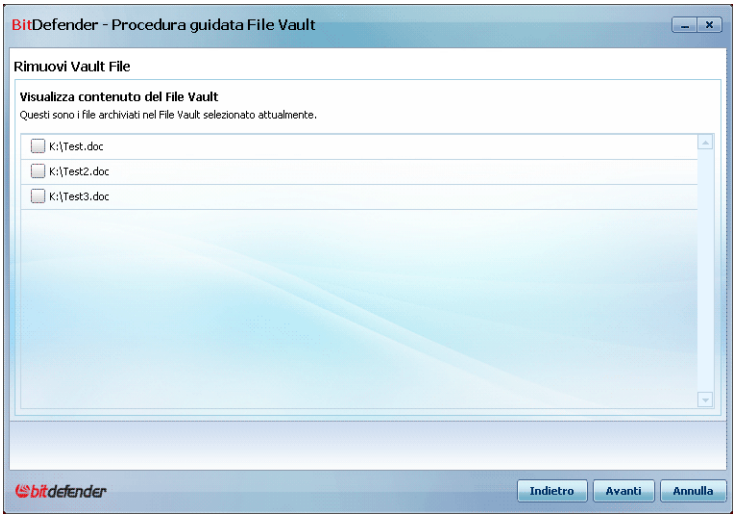


Conferma password

Digitare la password nel campo corrispondente e cliccare su **Avanti**.

Passo 3/5 - Selezionare file

Qui è dove vi verrà chiesta la lista dei file del vault selezionato in precedenza.

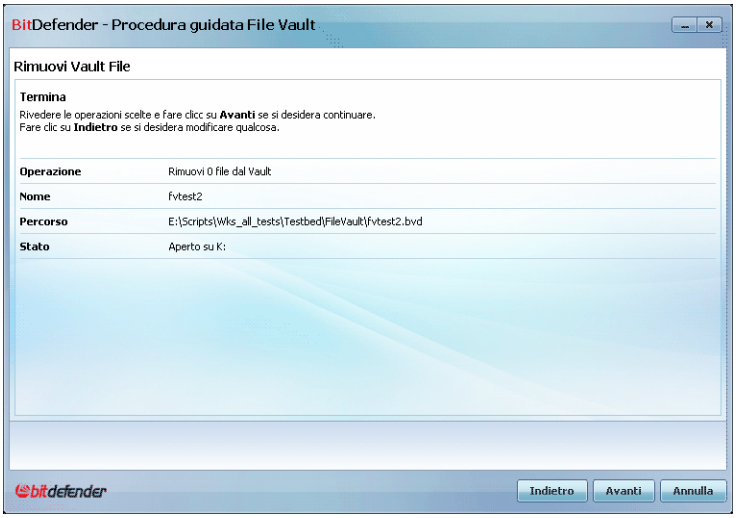


Seleziona file

Selezionare i file da rimuovere e cliccare su **Avanti**.

Passo 4/5 - Sommario

Qui è dove potrete rivedere le operazioni selezionate.

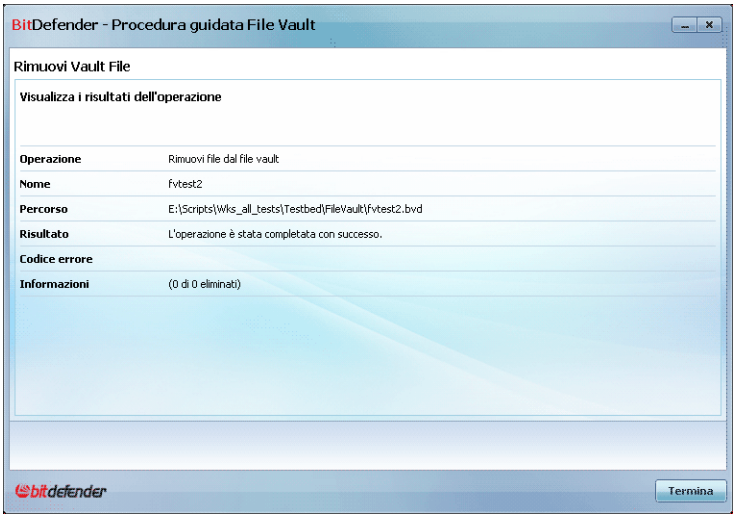


Riassunto

Selezionare **Avanti**.

Passo 5/5 – Risultati

Qui potete vedere il risultato dell'operazione.



Risultati

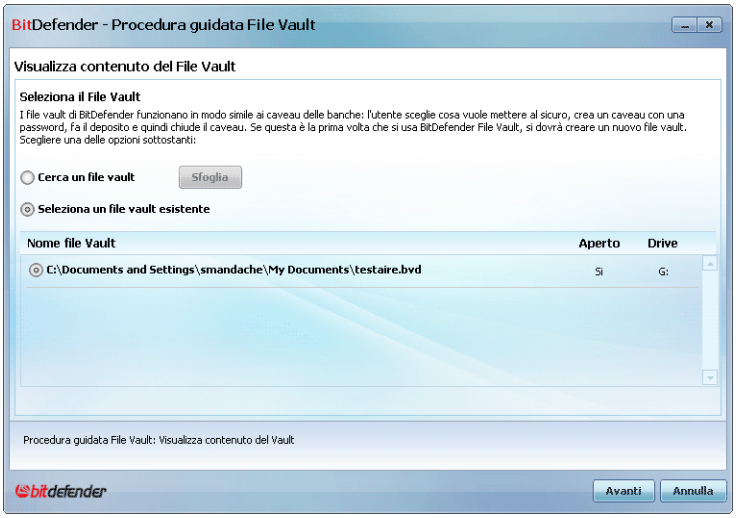
Selezionare **Termina**.

11.6.3. Visualizza File Vault

Questo assistente permette di aprire uno specifico file vault e visualizzare i file al suo interno.

Passo 1/4 - Selezionare Vault

Qui potete specificare il vault dal quale visualizzare i file.


BitDefender - Procedura guidata File Vault
Visualizza contenuto del File Vault
Seleziona il File Vault
I file vault di BitDefender funzionano in modo simile ai caveau delle banche: l'utente sceglie cosa vuole mettere al sicuro, crea un caveau con una password, fa il deposito e quindi chiude il caveau. Se questa è la prima volta che si usa BitDefender File Vault, si dovrà creare un nuovo file vault. Scegliere una delle opzioni sottostanti:
Cerca un file vault
Sfoglia
Seleziona un file vault esistente
Nome file Vault
Aperto
Drive
C:\Documents and Settings\smandache\My Documents\testaire.bvd
Si
G:
Procedura guidata File Vault: Visualizza contenuto del Vault
bitdefender
Avanti
Annulla

Seleziona Vault

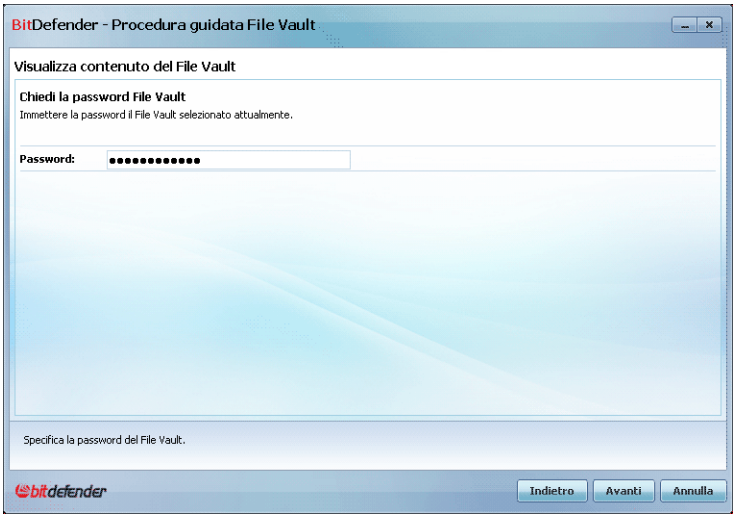
Se selezionate **Trovare un Vault File**, dovete cliccare su **Sfoglia** e selezionare il vault. Dovrete andare al passo 3 se il vault selezionato è aperto (montato) o al passo 2 se è bloccato (smontato).

Se cliccate su **Selezionare un Vault esistente**, dovrete poi cliccare sul nome del vault desiderato. Dovrete andare al passo 3 se il vault selezionato è aperto (montato) o al passo 2 se è bloccato (smontato).

Selezionare **Avanti**.

Passo 2/4 - Password

Qui è dove vi verrà chiesto di inserire la password per il vault selezionato.

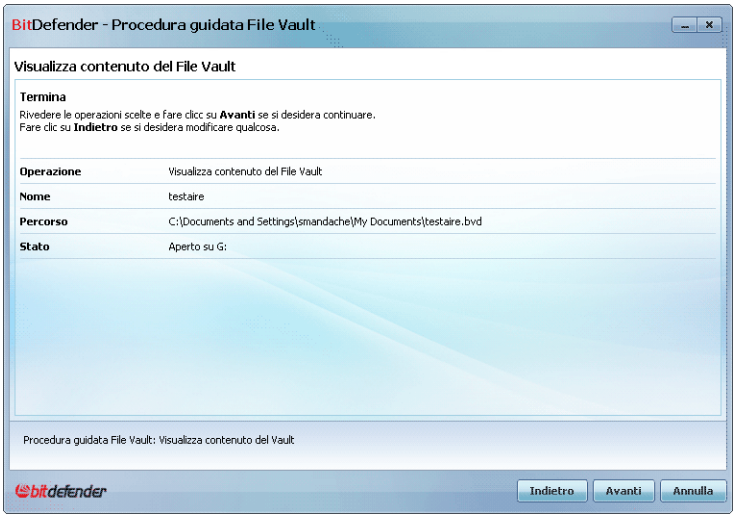


Conferma password

Digitare la password nel campo corrispondente e cliccare su **Avanti**.

Passo 3/4 - Sommario

Qui è dove potrete rivedere le operazioni selezionate.

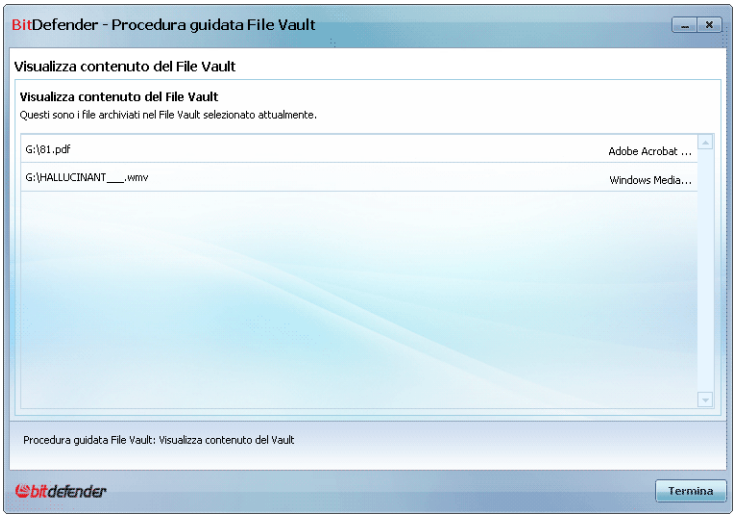


Riassunto

Selezionare **Avanti**.

Passo 4/4 – Risultati

Qui è dove potete visualizzare i file del vault.



Risultati

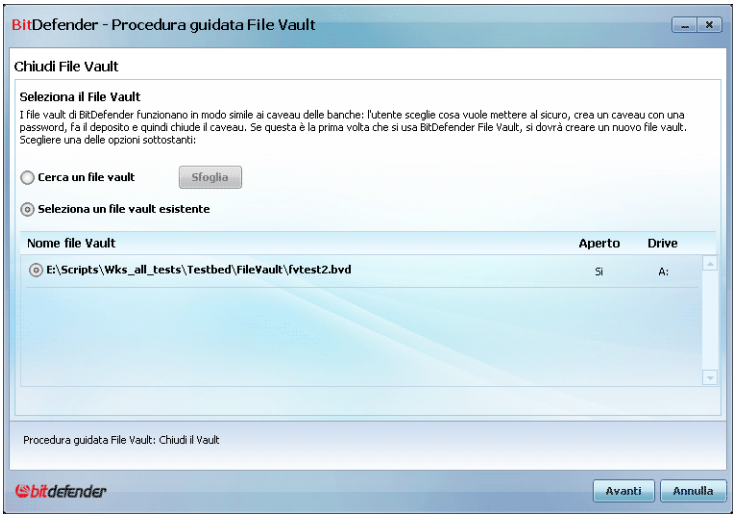
Selezionare **Termina**.

11.6.4. Blocca File Vault

Questo assistente permette di bloccare uno specifico file vault per proteggere il suo contenuto.

Passo 1/3 - Selezionare Vault

Qui potete specificare il vault da bloccare.


BitDefender - Procedura guidata File Vault
Chiudi File Vault
Seleziona il File Vault
I file vault di BitDefender funzionano in modo simile ai caveau delle banche: l'utente sceglie cosa vuole mettere al sicuro, crea un caveau con una password, fa il deposito e quindi chiude il caveau. Se questa è la prima volta che si usa BitDefender File Vault, si dovrà creare un nuovo file vault. Scegliere una delle opzioni sottostanti:
Cerca un file vault
Sfoglia
Seleziona un file vault esistente
Nome file Vault
Aperto
Drive
E:\Scripts\Wks_all_tests\Testbed\FileVault\fvtest2.bvd
Si
A:
Procedura guidata File Vault: Chiudi il Vault
bitdefender
Avanti
Annulla

Seleziona Vault

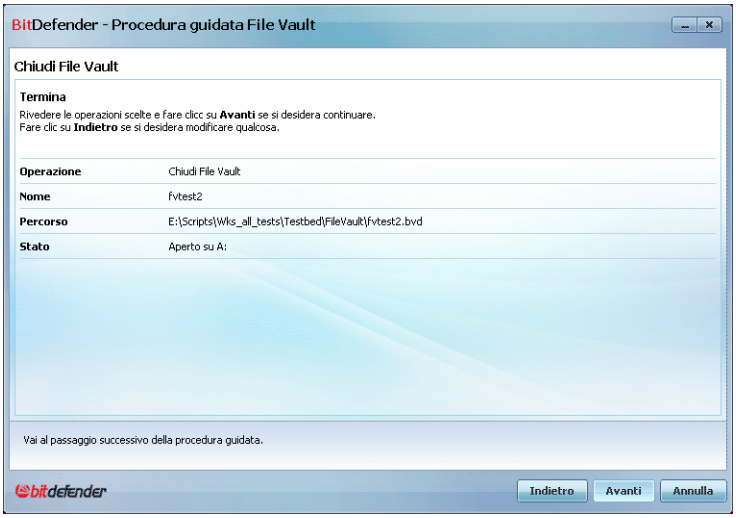
Se selezionate **Cercare un Vault File**, dovete cliccare su **Sfoglia** e selezionare il vault.

Se cliccate su **Selezionare un Vault File esistente** dovrete poi cliccare sul nome del vault desiderato.

Selezionare **Avanti**.

Passo 2/3 - Sommario

Qui è dove potrete rivedere le operazioni selezionate.

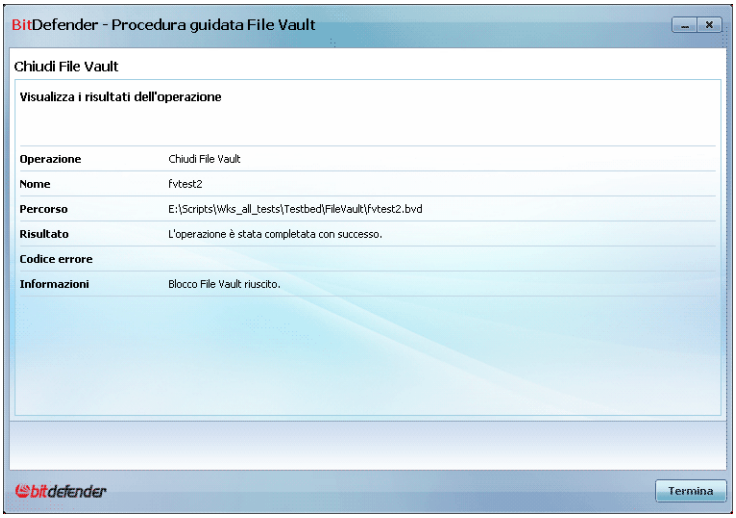


Riassunto

Selezionare **Avanti**.

Passo 3/3 – Risultati

Qui potete vedere il risultato dell'operazione.



Risultati

Selezionare **Termina**.

Modalità intermedia

12. Dashboard

La scheda Dashboard fornisce informazioni sullo stato di sicurezza del computer e permette di risolvere i problemi in sospeso.

BitDefender Total Security 2010
Impostazioni
DASHBOARD
SICUREZZA
OTTIMIZZATORE
ARCHIVIO FILE
RETE
Stato di Sicurezza
Profilo di Utilizzo: Personalizzato
Aggiorna ora
AVVISO: 1 problema influenza lo stato di sicurezza di questo PC.
Risolvi tutto
Informazioni sullo stato
SICUREZZA
ALLARME CRITICO - 1 problema in sospeso
OTTIMIZZATORE
NON MONITORATO - Nessuna informazione disponibile
ARCHIVIO FILE
NON MONITORATO - Nessuna informazione disponibile
RETE
NON CONFIGURATO - Questo modulo è disabilitato.
Il modulo dashboard visualizza lo stato della sicurezza del prodotto oltre a i link ai più importanti moduli di prodotti.
bitdefender
Rinnova Registra Ora Supporto Aiuto Visualizza registri

Dashboard

La Dashboard è costituita dalle seguenti sezioni:

- **Stato Generale** - Indica il numero di problemi che influiscono sul computer ed aiuta a risolverli. Se vi sono problemi in sospeso verrà visualizzato un **cerchio rosso con un punto esclamativo** e il pulsante **Risolvi Tutti i Problemi**. Fare clic sul pulsante per avviare l'assistente Risolvi Tutti i Problemi.
- **Dettagli Stato** - Indica lo stato di ciascun modulo principale utilizzando frasi esplicite e una delle seguenti icone:

  Cerchio verde con un segno di spunta: Non vi sono problemi che influenzano lo stato di sicurezza. Il computer e i dati sono protetti.

  Cerchio grigio con un punto esclamativo: L'attività dei componenti di questo modulo non viene monitorata. Di conseguenza non vi sono informazioni disponibili sullo stato di sicurezza di tali componenti. Potrebbero esservi problemi specifici relativi a questo modulo.

  Cerchio blu con lettera i: E' necessario compiere alcune attività per ottimizzare il sistema o proteggere i dati.

Cerchio rosso con un punto esclamativo: Vi sono problemi che influiscono sulla sicurezza del sistema. I problemi critici richiedono immediata attenzione. Anche i problemi non critici dovrebbero essere affrontati il più presto possibile.

Fare clic sul nome di un modulo per visualizzare ulteriori dettagli sul suo stato e per configurare il monitoraggio dello stato dei suoi componenti.

- **Profilo di Utilizzo** - Indica il profilo di utilizzo attualmente selezionato e offre link alle attività collegate a tale profilo:
  - Quando è selezionato il profilo **Tipico** il pulsante **Scansione Ora** permettere di compiere una scansione del sistema utilizzando l'Assistente Scansione Antivirus. Verrà esaminato l'intero sistema, con l'eccezione degli archivi. Nella configurazione di default, viene effettuata la scansione alla ricerca di tutti i tipi di malware eccettuati i rootkit.
  - Quando è selezionato il profilo **Genitori** il pulsante **Controllo Genitori** permette di configurare le impostazioni di Controllo Genitori. Per ulteriori informazioni sulla configurazione del Controllo Genitori, fare riferimento a «*Controllo genitori*» (p. 222).
  - Quando viene selezionato il profilo **Giocatore** il pulsante **Attiva/disattiva Modalità Gioco** permette di attivare/disattivare la Modalità Gioco. La Modalità Gioco modifica temporaneamente le impostazioni di protezione in modo di minimizzare l'impatto sulle prestazioni del sistema.
  - Quando è selezionato il profilo **Personalizzato** il pulsante **Aggiorna Ora** avvia un aggiornamento immediato. Apparirà una nuova finestra, dove potrete visualizzare lo stato dell'aggiornamento.

  Se si desidera passare ad un profilo differente oppure modificare il profilo attualmente in uso, fare clic sul profilo e seguire l'assistente di configurazione.

13. Sicurezza

BitDefender contiene un modulo di Sicurezza che vi aiuta a mantenere il vostro BitDefender aggiornato ed il vostro computer libero di virus. Per accedere al modulo Sicurezza, cliccare sulla linguetta **Sicurezza**.

Sicurezza

Il modulo Sicurezza ha due sezioni:

- **Area di Stato** - Visualizza lo stato attuale di tutti i componenti di sicurezza monitorati e permette di selezionare quali componenti monitorare.
- **Attività Veloci** - Qui si trovano i collegamenti alle attività di sicurezza più importanti: aggiornamento immediato, scansione documenti, scansione del sistema, scansione appprofondita del sistema, scansione personalizzata, scansione vulnerabilità e controllo genitori.

13.1. Area di Stato

L'area di stato è l'area in cui può essere visualizzato l'elenco completo dei componenti di sicurezza controllati e del loro stato attuale. Controllando ogni modulo di sicurezza BitDefender informerà non solo quando vengono configurate impostazioni che possono influenzare la sicurezza del computer ma anche quando vengono dimenticate attività importanti.

Lo stato attuale di un componente è indicato utilizzando frasi esplicite e una delle icone seguenti:

Cerchio verde con un segno di spunta: Nessun problema riscontrato sul componente.

Cerchio rosso con un punto esclamativo: Alcuni problemi riscontrati sul componente.

Le frasi di descrizione dei problemi sono visualizzate in rosso. Fare clic sul pulsante **Risolvi** corrispondente ad una frase per risolvere il problema riportato. Se un problema non viene risolto subito seguire l'assistente per risolverlo.

13.1.1. Configurazione del Monitoraggio Stato

Per selezionare i componenti che BitDefender deve monitorare, fare clic su **Configura Controllo Stato** e selezionare la casella di controllo **Abilita allarmi** corrispondente alle caratteristiche che si desidera monitorare.

Importante

E' necessario abilitare il controllo dello stato di un componente se si desidera ricevere notifiche quando vi sono problemi che influenzano la sicurezza di tale componente. Per assicurarsi che il sistema sia completamente protetto abilitare il monitoraggio per tutti i componenti e risolvere tutti i problemi riportati.

BitDefender può monitorare lo stato dei seguenti componenti di sicurezza:

- **Antivirus** - BitDefender controlla lo stato dei due componenti della funzione Antivirus: protezione in tempo reale e scansione a richiesta. I problemi più comuni riportati per questo componente vengono elencati nella seguente tabella.

Problema	Descrizione
La protezione in tempo reale è disabilitata	I file non vengono controllati quando viene effettuato l'accesso da parte vostra o da parte di un'applicazione in esecuzione sul sistema.
Non è mai stata eseguita la scansione del computer alla ricerca di malware	Non è mai stata compiuta una scansione del sistema su richiesta per controllare che i file contenuti sul computer siano esenti da malware.
L'ultima scansione di sistema avviata è stata annullata prima della sua conclusione	È stata avviata, ma non completata, una scansione completa del sistema.

Problema	Descrizione
L'Antivirus è in uno stato critico	La protezione in tempo reale del sistema è disabilitata e la scansione del sistema è ormai necessaria da lungo tempo.

- **Aggiornamento** - BitDefender controlla se le firme del malware sono aggiornate. I problemi più comuni riportati per questo componente vengono elencati nella seguente tabella.

Problema	Descrizione
L'Aggiornamento Automatico è disabilitato	Le firme del malware del prodotto BitDefender non vengono aggiornate automaticamente e regolarmente.
L'aggiornamento non è stato compiuto per x giorni	Le firme del malware del prodotto BitDefender sono obsolete.

- **Firewall** - BitDefender controlla lo stato della funzione Firewall. Se non è abilitata, verra riportato il problema **Firewall disabilitato**.
- **Antispam** - BitDefender controlla lo stato della funzione Antispam. Se non è abilitata, verra riportato il problema **Antispam disabilitato**.
- **Antiphishing** - BitDefender controlla lo stato della funzione di Antiphishing. Se non è abilitata per tutte le applicazioni supportate, verrà riportato il problema **Antiphishing disabilitato**.
- **Controllo Genitori** - BitDefender controlla lo stato della funzione Controllo Genitori. Se non è abilitata, verra riportato il problema **Controllo Genitori non configurato**.
- **Controllo Vulnerabilità** - BitDefender tiene traccia della funzione Controllo Vulnerabilità. Controllo Vulnerabilità comunica all'utente la necessità di installare aggiornamenti di Windows, aggiornamenti dell'applicazione e se è necessario rinforzare alcune password.

  I problemi più comuni riportati per questo componente vengono elencati nella seguente tabella.

Stato	Descrizione
Controllo Vulnerabilità è disabilitato	BitDefender non controlla potenziali vulnerabilità relative ad aggiornamenti di Windows mancanti, aggiornamenti delle applicazioni o password deboli.

Stato	Descrizione
Sono state individuate molteplici vulnerabilità	BitDefender ha trovato aggiornamenti di Windows/di applicazioni mancanti e/o password deboli.
Aggiornamenti critici Microsoft	Sono disponibili aggiornamenti di Windows critici, ma non sono stati installati.
Altri aggiornamenti Microsoft	Sono disponibili aggiornamenti di Windows non critici, ma non sono stati installati.
L'aggiornamento automatico di Windows è disabilitato	Gli aggiornamenti automatici di Windows non vengono automaticamente installati man mano che divengono disponibili.
Applicazione (obsoleta)	È disponibile una nuova versione dell'Applicazione ma non è stata installata.
Utente (Password Debole)	Individui malintenzionati possono individuare una password utente utilizzando software speciale.

13.2. Funzioni Veloci

In questo elenco è possibile trovare dei link alle attività di sicurezza più importanti:

- **Aggiorna adesso** - inizia un aggiornamento immediato.
- **Scansione del Sistema** - avvia una scansione completa del computer (archivi esclusi). Per ulteriori attività di scansione a richiesta, fare clic su su questo pulsante e selezionare un'attività di scansione differente: Scansione Documenti o Scansione Approfondita del Sistema.
- **Scansione Personalizzata** - avvia un assistente che permette di creare ed eseguire un'attività di scansione personalizzata.
- **Scansione Vulnerabilità** - avvia una procedura guidata che controlla il sistema alla ricerca di vulnerabilità ed aiuta a risolverle.
- **Configura Genitori** - apre la finestra di configurazione Controllo Genitori.

13.2.1. Aggiornamento di BitDefender

Tutti giorni vengono trovati ed identificati nuovi malware. E' quindi molto importante mantenere aggiornato il vostro BitDefender con le impronte più recenti del malware.

Di default, BitDefender controlla se ci sono aggiornamenti quando accendete il computer ed in seguito **ogni ora**. Ad ogni modo, se si vuole aggiornare BitDefender, cliccare semplicemente su **Aggiorna adesso**. Il processo di aggiornamento verrà iniziato ed apparirà immediatamente la seguente finestra:

BitDefender Total Security 2010
Aggiorna
Aggiorna BitDefender
BitDefender controllerà gli ultimi file e li aggiornerà automaticamente. Assicurarsi di avere una connessione internet prima di eseguire questa attività. Si consiglia vivamente di mantenere BitDefender aggiornato per garantire la sicurezza del sistema.
Stato: No
Aggiornamento totale: 19 KB
Scaricati: 19 KB
L'ultimo aggiornamento è stato installato con successo.
Per avere maggiori informazioni su ogni opzione mostrata nell'Interfaccia Utente di BitDefender, muovere il mouse sulla finestra. Un testo di aiuto dettagliato verrà visualizzato in questa area.
Annulla
Indietro
Termina

Aggiornamento di BitDefender

In questa finestra potete visualizzare lo stato del processo di aggiornamento.

Il processo di aggiornamento viene eseguito in volo, il chè vuol dire che i file da aggiornare vengono sostituiti progressivamente. In questo modo, il processo di aggiornamento non interesserà l'operatività del prodotto, nello stesso tempo, ogni vulnerabilità verrà esclusa.

Se si desidera chiudere questa finestra, cliccare semplicemente su **Annulla**. Ad ogni modo, questo non fermerà il processo di aggiornamento.

Nota
Se siete connessi a Internet mediante una connessione telefonica, è consigliato l'aggiornamento periodico di BitDefender su richiesta dell'utente.

Riavviare il computer se richiesto. In caso di un aggiornamento importante, verrà chiesto di riavviare il computer. Cliccare su **Riavviare** per riavviare il sistema immediatamente.

Se si desidera riavviare il sistema più tardi, cliccare semplicemente su **OK**. Si consiglia di riavviare il sistema al più presto.

13.2.2. Scansione con BitDefender

Per avviare la scansione del vostro computer alla ricerca di malware, eseguire un task particolare di scansione facendo clic sul pulsante corrispondente o

selezionandolo dal menu a tendina. La seguente tabella elenca i task di scansione disponibili, assieme alla loro descrizione:

Task	Descrizione
Scansione sistema	Esamina l'intero sistema, esclusi gli archivi. Nella configurazione di default la scansione ricerca tutti i tipi di malware ad eccezione dei rootkit.
Scansione Documenti	Usare questa funzione per esaminare le cartelle importanti dell'utente corrente: `Documenti`, `Desktop` e `Avvio`. Questo garantirà la sicurezza dei vostri documenti, uno spazio di lavoro sicuro e l'esecuzione di applicazioni pulite all'avvio.
Scansione del Sistema approfondita	Esamina l'intero sistema. Nella configurazione predefinita, esegue la scansione per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.
Personalizzare Scansione	Usare questa funzione per scegliere file e cartelle specifici da esaminare.

Nota

Poiché le funzioni **Scansione approfondita del sistema** e **Scansione completa del sistema** analizzano l'intero sistema, la scansione può richiedere un po' di tempo. Quindi consigliamo di eseguire questi compiti con priorità bassa o, meglio, quando il sistema è inattivo.

Quando si esegue una Scansione del Sistema, Scansione Approfondita del Sistema o Scansione Documenti, apparirà l'assistente Scansione Antivirus. Seguire la procedura di tre passi per completare il processo di scansione. Per ulteriori informazioni sulla procedura guidata, far riferimento a «*Procedura guidata scansione antivirus*» (p. 57).

Quando si esegue una Scansione Personalizzata, l'assistente Scansione Personalizzata vi condurrà lungo il processo di scansione. Seguire i sei passi della procedura guidata per effettuare la scansione di file o cartelle specifiche. Per ulteriori informazioni sulla procedura guidata, far riferimento a «*Assistente Scansione Personalizzata*» (p. 62).

13.2.3. Ricerca delle Vulnerabilità

La Scansione delle Vulnerabilità controlla gli Aggiornamenti di Microsoft Windows, di Microsoft Windows Office e le password dei tuoi account di Microsoft Windows per assicurare che il tuo Sistema Operativo sia aggiornato e che le password non siano vulnerabili.

Per controllare il vostro computer alla ricerca di vulnerabilità, cliccare su **Scansione Vulnerabilità** e seguire i sei passi della procedura guidata. Per ulteriori informazioni fare riferimento a «*Correggi Vulnerabilità*» (p. 280).

13.2.4. Configurazione Controllo Genitori

Il Controllo dei Genitori BitDefender vi permette di controllare l'accesso ad Internet e ad applicazioni specifiche di ogni utente che possieda un account nel sistema.

Per configurare il Controllo Genitori, fare clic su **Configura Genitori**. Apparirà una nuova finestra.

Configurazione Controllo Genitori BitDefender

Qui è possibile vedere lo stato del Controllo Genitori per ogni account utente di Windows ed è possibile configurare le regole del Controllo Genitori. Questa finestra di configurazione è simile alla scheda Controllo Genitori in Modalità Avanzata. Per ulteriori informazioni fare riferimento a «*Controllo genitori*» (p. 222).

14. Tune-Up

BitDefender è dotato di un modulo di Ottimizzazione che aiuta a mantenere l'integrità del sistema. Gli strumenti di manutenzione offerti sono fondamentali per il miglioramento della reattività del sistema e la gestione efficace dello spazio sul disco rigido.

Per eseguire operazioni di manutenzione sul PC, fare clic sulla scheda **Ottimizzazione** ed utilizzare gli strumenti forniti.

BitDefender Total Security 2010
Impostazioni
DASHBOARD
SICUREZZA
OTTIMIZZATORE
ARCHIVIO FILE
RETE
Funzioni Veloci
Pulisci il Registro
Ripristina il Registro
Distruggi file
Pulizia PC
Trova duplicati
Deframmenta i dischi
Stato
Il Pulitore del Registro non è mai stato eseguito
La Pulizia PC non è mai stata eseguita
Ricerca di file duplicati mai eseguita
La Deframmentazione del Disco non è mai stata eseguita
Esegui adesso
Configura il monitoraggio stato
Il modulo Ottimizzatore mostra lo stato degli strumenti di BitDefender creati per migliorare le performance del sistema, insieme ai link delle funzioni di ottimizzazione.
bitdefender
Rinnova Registra Ora Supporto Aiuto Visualizza registri

Tune-Up

Il modulo di Ottimizzazione è costituito da due sezioni:

- **Area di Stato** - Visualizza lo stato attuale dei componenti di ottimizzazione principali e permette di selezionare quali componenti monitorare.
- **Attività Veloci** - Qui è possibile trovare i link alle più importanti funzioni di ottimizzazione: pulizia e recupero del registro, eliminazione permanente dei file, eliminazione dei file temporanei di Internet e dei cookie, eliminazione dei file duplicati, deframmentazione dei dischi locali.

14.1. Area di Stato

Lo stato attuale di un componente è indicato utilizzando frasi esplicite e una delle icone seguenti:

Cerchio verde con un segno di spunta: Nessun problema riscontrato sul componente.
Cerchio blu con lettera i: Si consiglia di eseguire l'attività.

Per eseguire un'attività consigliata, fare clic sul pulsante **Esegui Ora** corrispondente e seguire l'assistente.

14.1.1. Configurazione del Monitoraggio Stato

Fare clic su **Configura Controllo Stato** e selezionare la casella di controllo **Abilita avvisi** corrispondente allo strumento di ottimizzazione che si desidera venga controllato da BitDefender.

BitDefender può monitorare lo stato dei seguenti strumenti di ottimizzazione:

- **Pulizia del Registro** - BitDefender tiene traccia del momento in cui è stato utilizzato per l'ultima volta questo strumento. Se l'esecuzione è stata rimandata troppo a lungo, verrà riportato il problema **Non è stata mai eseguita la Pulizia del Registro** / **La Pulizia del Registro non è stata eseguita per x giorni**.
- **Pulizia del PC** - BitDefender tiene traccia del momento in cui è stato utilizzato per l'ultima volta questo strumento. Se l'esecuzione è stata rimandata troppo a lungo, verrà riportato il problema **Non è stata mai eseguita la Pulizia del PC** / **La Pulizia del PC non è stata eseguita per x giorni**.
- **Ricercatore di Duplicati** - BitDefender tiene traccia del momento in cui è stato utilizzato per l'ultima volta questo strumento. Se l'esecuzione è stata rimandata troppo a lungo, verrà riportato il problema **Non è stato mai eseguito il Ricercatore di Duplicati** / **Il Ricercatore di Duplicati non è stato eseguito per x giorni**.
- **Deframmentazione Disco** - BitDefender tiene traccia del momento in cui è stato utilizzato per l'ultima volta questo strumento. Se l'esecuzione è stata rimandata troppo a lungo, verrà riportato il problema **Non è stata mai eseguita la Deframmentazione Disco** / **La Deframmentazione Disco non è stata eseguita per x giorni**.

Importante
Per migliorare le prestazioni del computer si consiglia di eseguire periodicamente tutte le attività.

14.2. Funzioni Veloci

Qui si possono trovare i collegamenti alle attività di ottimizzazione:

- Pulizia del Registro identifica ed elimina i riferimenti orfani o non validi nel Registro di Sistema di Windows. Per mantenere il Registro di Windows pulito ed ottimizzato si consiglia di eseguire la Pulizia del Registro mensilmente.

- Recupero del Registro può recuperare chiavi di registro cancellate precedentemente dal Registro di Sistema di Windows usando la Pulizia del Registro di BitDefender.
- Eliminazione definitiva dei File cancella in modo permanente i file e le loro tracce dal sistema.
- Pulizia PC rimuove i file temporanei di Internet ed i cookie, i file di sistema non utilizzati e i collegamenti a documenti recenti.
- Ricerca Duplicati trova ed elimina i file duplicati sul vostro sistema.
- Deframmentazione Dischi riorganizza fisicamente i dati sul disco rigido in modo che i frammenti di ogni file vengano conservati tutti insieme ed in maniera continua.

14.2.1. Pulizia del Registro di Windows

Il Registro di Windows è una parte importante dei sistemi operativi Windows. Esso è un database che contiene informazioni ed impostazioni per l'hardware ed il sistema operativo, applicazioni installate, utenti, preferenze del vostro computer ed altro.

Molte applicazioni scrivono delle chiavi nel Registro di Windows al momento dell'installazione. Quando tali applicazioni vengono rimosse, alcune delle chiavi di registro associate potrebbero non venire eliminate e rimanere nel Registro di Windows, rallentando il vostro sistema e causando addirittura instabilità nel sistema. La stessa cosa accade quando eliminate dei collegamenti o certi file di applicazioni installate nel vostro sistema, così come nel caso di driver corrotti.

Per pulire il Registro di Windows e migliorare le prestazioni del vostro sistema, utilizzare lo Strumento di Pulizia del Registro. Lo Strumento di Pulizia esamina il Registro di Windows ed elimina le chiavi di registro non valide.

Per pulire il Registro di Windows, seguire questi passaggi:

1. Fare clic su **Pulizia Registro**.
2. Seguire la procedura di quattro passaggi. Per ulteriori informazioni fare riferimento a «*Procedura guidata Pulitore Registro*» (p. 95).

14.2.2. Recupero di Registro Cancellato

A volte, dopo la pulizia del registro, potreste notare che il vostro sistema non lavora bene, o che alcune applicazioni non operano correttamente, a causa di chiavi di registro mancanti. Questo può essere causato da chiavi di registro condivise che sono state eliminate durante la pulizia del registro o da altre chiavi eliminate. Per risolvere questo problema dovete recuperare il registro pulito.

Importante
Solo gli utenti con diritti di amministrazione possono recuperare il registro pulito.

Per recuperare il registro pulito, seguire questi passaggi:

1. Fare clic su **Recupera Registro**.
2. Seguire la procedura di due passaggi. Per ulteriori informazioni fare riferimento a «*Procedura guidata Ripristino Registro*» (p. 100).

14.2.3. Trovare file duplicati

I file duplicati si mangiano lo spazio del vostro disco rigido. Pensate solo di avere lo stesso file `.mp3` salvato in tre ubicazioni diverse.

Per rilevare ed eliminare file duplicati dal vostro computer, potete utilizzare il Ricercatore di Duplicati. In questo modo potrete migliorare la gestione dello spazio libero sui vostri dischi rigidi.

Per trovare file duplicati sul vostro computer, seguire questi passaggi:

1. Fare clic su **Trova Duplicati**.
2. Seguire la procedura di quattro passaggi. Per ulteriori informazioni fare riferimento a «*Procedura guidata Ricercatore di Duplicati* » (p. 91).

14.2.4. Pulizia del vostro PC

Ogni volta che visitate una pagina web, vengono creati dei file temporanei Internet per permettervi un accesso più veloce la volta successiva. Nonostante vengono riferiti come temporanei, questi file non vengono eliminati quando chiudete il browser. Questo può diventare un problema di privacy poichè questi file possono essere visti da chiunque abbia accesso al vostro computer. Inoltre, con il tempo, questi file raggiungono una dimensione considerevole, mangiandosi lo spazio del vostro disco rigido.

Anche i cookies vengono immagazzinati nel vostro computer quando visitate una pagina web. I cookies son dei piccoli file contenenti informazioni sulle vostre preferenze di navigazione. Essi potrebbero essere visti anche come un problema di privacy, poichè possono essere analizzati ed usati dai pubblicisti per tracciare i vostri interessi e gusti on line.

La Pulizia del PC vi aiuta a liberare spazio su disco ed a proteggere la vostra privacy eliminando i file che non vi saranno più utili.

- File temporanei Interrnet e cookie di Internet Explorer.
- File temporanei Interrnet e cookie di Mozilla Firefox.
- file di sistema temporanei creati da Windows durante la sua operazione.
- collegamenti ai documenti recenti creati da Windows quando aprite un file.

Per pulire il sistema da file temporanei Internet e cookie, file di sistema temporanei e collegamenti a documenti recenti, seguire questi passaggi:

1. Fare clic su **Pulizia PC**.
2. Seguire la procedura guidata di tre passaggi. Per ulteriori informazioni fare riferimento a «*Procedura guidata pulizia PC*» (p. 88).

14.2.5. Eliminazione Definitiva dei File

Quando eliminate un file, non si può più accedere ad esso con i normali strumenti. Comunque, il file continua ad essere immagazzinato sul disco rigido finchè non verrà sovrascritto quando copierete nuovi file.

Anche se eliminate un file, esso può essere recuperato utilizzando dei programmi specializzati. Questo potrebbe rappresentare una minaccia alla vostra privacy, poichè ci potrebbero essere dei tentativi maligni di prendere i vostri dati privati.

Per evitare che i dati sensibili vengano recuperati dopo che li avete eliminati, potete utilizzare BitDefender per eliminarli definitivamente, rimuovendoli fisicamente dal vostro disco rigido.

Per eliminare definitivamente i file, seguire questi passaggi:

1. Fare clic su **Elimina definitivamente File**.
2. Seguire la procedura guidata di tre passaggi. Per ulteriori informazioni fare riferimento a «*Procedura guidata distruzione file*» (p. 102).

14.2.6. Deframmentazione dei Volumi del Disco Rigido.

Quando si copia un file che eccede il blocco più grande di spazio libero su disco rigido, si verifica una frammentazione del file. Siccome non c'è spazio libero sufficiente per immagazzinare l'intero file in modo continuo, verrà immagazzinato in diversi blocchi. Quando si accede al file frammentato, i suoi dati devono essere letti da diverse ubicazioni.

La frammentazione del file rallenta l'accesso allo stesso e diminuisce le prestazioni del sistema. Questo accellera anche l'usura del disco rigido.

Per ridurre la frammentazione dei file dovete deframmentare i dischi periodicamente. La deframmentazione fisica dei dischi riorganizza i dati sul disco rigido in modo che i pezzi di ogni file vengano immagazzinati assieme ed in modo continuo. Questo tenta anche di creare aree di spazio libero più grandi per evitare che i file vengano frammentati dopo.

Si consiglia di deframmentare il disco rigido per:

- accedere più velocemente ai file.
- migliorare le prestazioni del sistema in generale.
- prolungare la vita del disco rigido.

Per deframmentare il disco rigido, seguire questi passaggi:

1. Fare clic su **Deframmentazione Dischi**.

2. Seguire la procedura guidata di tre passaggi. Per ulteriori informazioni fare riferimento a «*Procedura guidata Deframmentazione Disco*» (p. 84).

Nota

La deframmentazione può impiegare un po' di tempo dal momento in cui implica lo spostamento di porzioni di dati immagazzinati da un posto all'altro del disco rigido. Vi consigliamo di eseguire la deframmentazione quando non state usando il vostro computer.

15. Archiviazione File

BitDefender contiene un modulo Archiviazione File che permette di mantenere i dati, non solo sicuri, ma anche confidenziali. Per conseguire questo obiettivo, effettuare il backup dei file e utilizzare la criptazione dei file.

Backup. La protezione antivirus da sola non è più sufficiente per proteggere i vostri dati di valore. Immaginate che il vostro sistema sia libero dai virus ma che per qualche motivo il computer si blocca proprio quando più ne avete bisogno. In questo caso la sezione di Backup del modulo Archiviazione File viene utile. E' possibile effettuare il backup dei dati in sicurezza con BitDefender.

Criptazione file. Sicuramente vorrete mantenere i vostri dati sensibili lontani da occhi indiscreti. In questo caso la sezione Criptazione File del modulo Archiviazione File viene utile. Con questa caratteristica è possibile proteggere i file inserendoli in file vault.

- Il file vault è uno spazio sicuro dove immagazzinare informazioni personali o file sensibili.
- Il file vault è un file criptato sul vostro computer con estensione bvd. Siccome è criptato, i dati al suo interno sono invulnerabili a furti o a violazioni di sicurezza.
- Quando aprite questo file bvd, apparirà una nuova partizione logica (un nuovo drive). Vi sarà più facile capire questo processo se pensate ad uno simile: aprire un'immagine ISO come CD virtuale.

  Aprire Risorse del Computer e vedrete un nuovo drive basato sulla vostra criptazione file. In esso sarete in grado di fare operazioni sui file (copiare, cancellare, modificare, etc). I file saranno protetti finchè risiederanno in questo drive (perchè viene richiesta una password per l'operazione di apertura).

  Quando avrete finito, bloccare (smontare) il file per comminciare a proteggere il suo contenuto.

Per accedere al modulo Archiviazione File, fare clic sulla scheda **Archiviazione File**.

Archiviazione File

Il modulo Archiviazione File contiene due sezioni:

- **Area di Stato** - Permette di visualizzare l'elenco completo dei componenti monitorati. È possibile scegliere quali componenti monitorare. Si consiglia di abilitare l'opzione di monitoraggio per tutti i componenti.
- **Attività Veloci** - Qui si trovano i link alle più importanti funzioni di sicurezza: backup e ripristino locale, aggiunta, visualizzazione e rimozione dei file nei vault, blocco dei file vault.

15.1. Area di Stato

Lo stato attuale di un componente è indicato utilizzando frasi esplicite e una delle icone seguenti:

Cerchio verde con un segno di spunta: Nessun problema riscontrato sul componente.
Cerchio rosso con un punto esclamativo: Alcuni problemi riscontrati sul componente.
Cerchio blu con lettera i: Si consiglia di eseguire l'attività.

Le frasi di descrizione dei problemi sono visualizzate in rosso. Fare clic sul pulsante **Risolvi** o sul pulsante **Esegui Ora** corrispondente ad una frase per risolvere il problema riportato. Se un problema non viene risolto subito seguire l'assistente per risolverlo.

Per selezionare i componenti che BitDefender deve monitorare, fare clic su **Configura Controllo Stato** e selezionare la casella di controllo **Abilita allarmi** corrispondente alle caratteristiche che si desidera monitorare.

L'area di stato della scheda Archiviazione File offre informazioni riguardanti lo stato dei seguenti componenti:

- **Criptazione File** controlla lo stato del File Vault. Se non è abilitata, verrà riportato il problema **Criptazione File disabilitata**.
- **Backup Locale** controlla lo stato della funzione Backup Locale. Se non è stato effettuato un backup dei dati per un periodo di tempo eccessivo, verrà riportato il problema **Non è mai stato eseguito il backup locale dei dati** / **Il backup locale dei dati non è stato eseguito in x giorni**.

15.2. Funzioni Veloci

Sono disponibili i seguenti tasti:

- **Backup locale** - Inizia la procedura che vi permette di fare delle copie di riserva dei dati di valore sul vostro computer, su CD, una ubicazione di rete o un altro disco rigido. Per ulteriori informazioni fare riferimento a «*Assistente Backup Locale*» (p. 76)
- **Ripristino locale** - Inizia la procedura che vi permette di ripristinare dei dati previamente salvati (backup) sul vostro computer, su CD, una ubicazione di rete o un altro disco rigido. Per accedere a questa attività, fare clic sulla del pulsante **Backup Locale**. Per ulteriori informazioni fare riferimento a «*Assistente Recupero Locale*» (p. 81)
- **Aggiungere File alla Criptazione** - inizia la procedura guidata che vi permette di immagazzinare i vostri file / documenti importanti privatamente mediante la loro criptazione in speciali drive protetti. Per ulteriori informazioni fare riferimento a «*Aggiungi file alla Criptazione (Vault)*» (p. 106).
- **Rimuovere File dalla Criptazione** - inizia la procedura guidata che vi permette di cancellare dati dai file protetti. Per ulteriori informazioni fare riferimento a «*Rimuovi Vault File*» (p. 111).
- **Visualizzare File Vault** - inizia la procedura guidata che vi permette di visualizzare il contenuto dei file vault. Per ulteriori informazioni fare riferimento a «*Visualizza File Vault*» (p. 116).
- **Bloccare File Vault** - inizia la procedura guidata che permette di bloccare un file vault per iniziare a proteggere il suo contenuto. Per ulteriori informazioni fare riferimento a «*Blocca File Vault*» (p. 120).

16. Rete

Il modulo Rete vi permette gestire i prodotti BitDefender installati sui computer di casa da un singolo computer. Per accedere al modulo Rete, fare clic sulla scheda **Rete**.

BitDefender Total Security 2010
Impostazioni
DASHBOARD
SICUREZZA
OTTIMIZZATORE
ARCHIVIO FILE
RETE
Funzioni Veloci
Abilita Rete domesti
Il modulo Rete mostra la struttura della rete domestica BitDefender (in grigio se la rete locale non è configurata). Fare clic su Abilita Rete per iniziare a configurare la rete domestica.
bitdefender
Rinnova Registra Ora Supporto Aiuto Visualizza registri

Rete

Per essere in grado di gestire i prodotti BitDefender installati sui computer di casa, dovete seguire questi passaggi:

1. Unirvi alla rete domestica BitDefender sul vostro computer. Unirsi alla rete consiste in configurare una password di amministrazione per la gestione della rete domestica.
2. Andare su ogni computer che si vuole gestire ed aggiungerli alla rete (impostare la password).
3. Tornare al vostro computer ed aggiungere i computer che volete gestire.

16.1. Funzioni Veloci

Inizialmente, solo un tasto sarà disponibile.

- **Abilita Rete** - permette di impostare una password di rete, pertanto creando e accedendo ad una rete.

Dopo aversi unito alla rete, appariranno molti più tasti.

- **Disabilita Rete** - permette di lasciare la rete.
- **Aggiungi Computer** - permette di aggiungere computer alla rete.
- **Esaminare Tutti** - vi permette di eseguire la scansione su tutti i computer in gestione contemporaneamente.
- **Aggiornare Tutti** vi permette di aggiornare tutti i computer in gestione contemporaneamente.
- **Registrare Tutti** vi permette di registrare tutti i computer in gestione contemporaneamente.

16.1.1. Unirsi alla Rete BitDefender

Per unirsi alla rete domestica BitDefender, seguire questi passaggi:

1. Fare clic su **Abilita rete**. Vi verrà chiesto di configurare le password per la gestione domestica.

BitDefender
Digitare password rete domestica
E' richiesta una password per accedere o creare una rete per motivi di sicurezza. Questa password proteggerà l'accesso al computer attraverso la rete domestica.
Password:
Reinserisci password:
OK
Annulla

Configurare Password

2. Inserire la stessa password in ognuno dei campi corrispondenti.
3. Selezionare **OK**.

Potete vedere il nome del computer apparire nella mappa della rete.

16.1.2. Aggiungere dei computer alla Rete BitDefender

Prima di poter aggiungere un computer alla rete domestica BitDefender dovrete configurare la password per la gestione domestica BitDefender sul rispettivo computer.

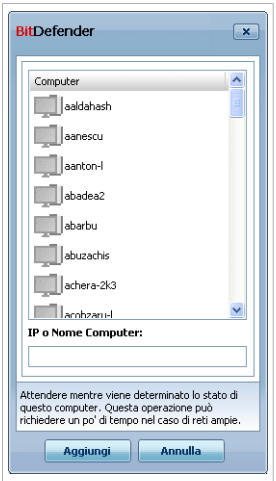
Per aggiungere un computer alla rete domestica BitDefender , seguire questi passi:

1. Fare clic su **Aggiungi Computer**. Vi verrà chiesto di fornire la password per la gestione domestica locale.

BitDefender
Inserire qui la password impostata quando è stata abilitata la Gestione domestica su questo PC.
Password
Non mostrare più questo messaggio durante questa sessione.
OK
Annulla

Inserire Password

2. Digitare la password per la gestione domestica e cliccare su **OK**. Apparirà una nuova finestra.



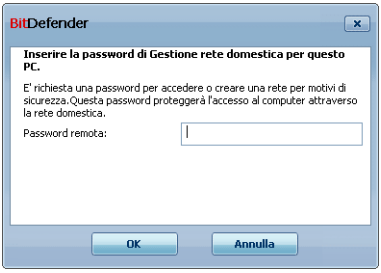
Aggiungi Computer

Potete vedere l'elenco dei computer in questa rete. Il significato dell'icona è il seguente:

Indica un computer online senza prodotti BitDefender installati.
Indica un computer online con BitDefender installato.
Indica un computer offline con BitDefender installato.

3. Eseguire una delle seguenti azioni:
   - Selezionare dall'elenco il nome del computer da aggiungere.
   - Digitare l'indirizzo IP o il nome del computer da aggiungere nel campo corrispondente.

4. Selezionare **Aggiungi**. Vi verrà chiesto di fornire la password per la gestione domestica sul rispettivo computer.


BitDefender
Inserire la password di Gestione rete domestica per questo PC.
E' richiesta una password per accedere o creare una rete per motivi di sicurezza. Questa password proteggerà l'accesso al computer attraverso la rete domestica.
Password remota:
OK
Annulla

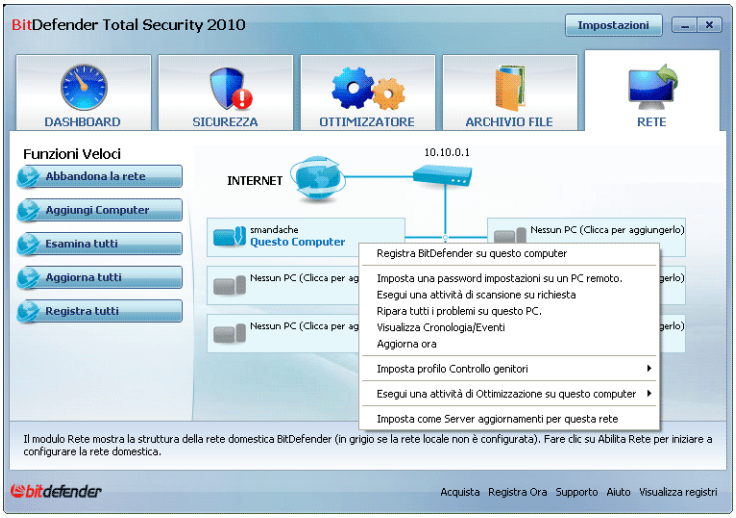
Autenticare

5. Digitare la password per la gestione domestica configurata sul rispettivo computer.
6. Selezionare **OK**. Se avete fornito la password corretta, il nome del computer selezionato apparirà nella mappa di rete.

Nota
Potete aggiungere fino a cinque computer alla mappa di rete.

16.1.3. Gestione della Rete BitDefender

Una volta che avete creato con successo una rete domestica BitDefender, potrete gestire tutti i prodotti BitDefender da un singolo computer.


BitDefender Total Security 2010
Impostazioni
DASHBOARD
SICUREZZA
OTTIMIZZATORE
ARCHIVIO FILE
RETE
Funzioni Veloci
Abbandona la rete
Aggiungi Computer
Esamina tutti
Aggiorna tutti
Registra tutti
INTERNET
10.10.0.1
smandache
Questo Computer
Nessun PC (Clicca per aggiungerlo)
Registra BitDefender su questo computer
Imposta una password impostazioni su un PC remoto.
Esegui una attività di scansione su richiesta
Ripara tutti i problemi su questo PC.
Visualizza Cronologia/Eventi
Aggiorna ora
Imposta profilo Controllo genitori
Esegui una attività di Ottimizzazione su questo computer
Imposta come Server aggiornamenti per questa rete
Il modulo Rete mostra la struttura della rete domestica BitDefender (in grigio se la rete locale non è configurata). Fare clic su Abilita Rete per iniziare a configurare la rete domestica.
bitdefender
Acquista Registra Ora Supporto Aiuto Visualizza registri

Mappa di rete

Se muovete il cursore su un computer nella mappa di rete, potete vedere una breve informazione su di esso (nome, indirizzo IP, numero di problemi che colpiscono la sicureza del sistema, stato della registrazione di BitDefender).

Se si fa clic con il pulsante destro sul nome del computer nella mappa di rete, è possibile vedere tutte le funzioni di amministrazione che si possono eseguire dal computer remoto.

- **Rimuovi il PC dalla rete domestica**

  Permette di rimuovere il PC dalla rete.

- **Registra BitDefender su questo computer**

  Permette di registrare BitDefender sul computer inserendo una chiave di licenza.

- **Stabilire una password per le impostazioni su un PC remoto**

  Permette di creare una password per limitare l'accesso alle impostazioni BitDefender sul PC.

- **Eseguire una attività di scansione su richiesta**

  Permette di eseguire una scansione a richiesta sul computer remoto. E' possibile compiere una qualsiasi delle seguenti attività di scansione: Scansione Documenti, Scansione del Sistema o Scansione del Sistema Approfondita.

- **Risolvere tutti i problemi su questo computer**

Permette di risolvere i problemi che influenzano la sicurezza del computer seguendo l'assistente Risolvi Tutti i Problemi.

- **Visualizzare Cronologia/Eventi**

  Permette di accedere al modulo **Cronologia&Eventi** del prodotto BitDefender installato sul computer.

- **Aggiorna adesso**

  Avvia il processo di aggiornamento per il prodotto BitDefender installato sul computer.

- **Imposta Profilo Controllo genitori**

  Permette di impostare la categoria di età da utilizzare per il filtro web del Controllo Genitori del computer: bambino, adolescente o adulto.

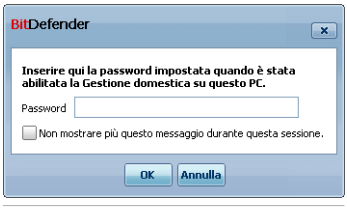
- **Esegui una funzione di Ottimizzazione su questo computer**

  Permette di eseguire un'attività di ottimizzazione sul PC remoto. E' possibile eseguire una delle seguenti attività: deframmentazione dischi o pulizia dei file temporanei di Internet.

- **Impostare come Server di aggiornamento per questa rete**

  Permette di impostare il computer come server di aggiornamento per tutti i prodotti BitDefender installati sui computer della rete. Utilizzando questa opzione si ridurrà il traffico Internet, poiché un solo computer della rete si collegherà ad Internet per scaricare gli aggiornamenti.

Prima di eseguire una funzione su un particolare computer, vi verrà chiesto di fornire la password per la gestione domestica locale.


BitDefender
Inserire qui la password impostata quando è stata abilitata la Gestione domestica su questo PC.
Password
Non mostrare più questo messaggio durante questa sessione.
OK
Annulla

Inserire Password

Digitare la password per la gestione domestica e cliccare su **OK**.

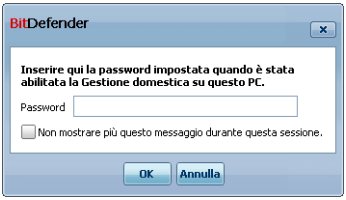
Nota

Se si ha in programma di eseguire diverse funzioni, è possibile selezionare **Non mostrare di nuovo questo messaggio durante questa sessione**. Selezionando questa opzione non vi verrà più chiesta la password durante la sessione corrente.

16.1.4. Scansione di tutti i computer

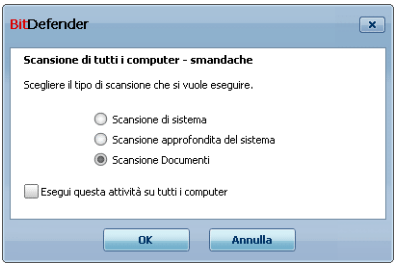
Per esaminare tutti i computer in gestione, seguire questi passaggi:

1. Cliccare su **Esaminare Tutti**. Vi verrà chiesto di fornire la password per la gestione domestica locale.


BitDefender
Inserire qui la password impostata quando è stata abilitata la Gestione domestica su questo PC.
Password
Non mostrare più questo messaggio durante questa sessione.
OK
Annulla

Inserire Password

2. Selezionare un tipo di scansione.
   - **Scansione del Sistema** - inizia una scansione completa del computer (archivi esclusi).
   - **Scansione Approfondita del Sistema** - inizia una scansione completa del computer (archivi inclusi).
   - **Scansione Documenti** - inizia una scansione veloce dei documenti e delle impostazioni.



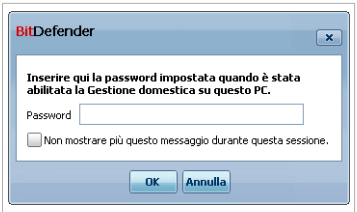
Selezionare tipo di scansione

3. Selezionare **OK**.

16.1.5. Aggiornamento di tutti i Computer

Per aggiornare tutti i computer in gestione, seguire questi passaggi:

1. Cliccare su **Aggiornare Tutti**. Vi verrà chiesto di fornire la password per la gestione domestica locale.


BitDefender
Inserire qui la password impostata quando è stata abilitata la Gestione domestica su questo PC.
Password
Non mostrare più questo messaggio durante questa sessione.
OK
Annulla

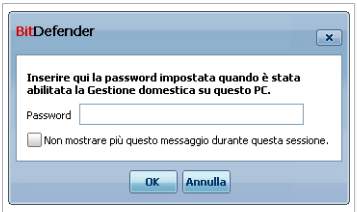
Inserire Password

2. Selezionare **OK**.

16.1.6. Registrazione di Tutti i Computer

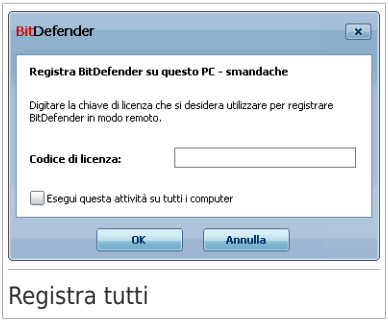
Per registrare tutti i computer in gestione, seguire questi passaggi:

1. Cliccare **Registrare Tutti**. Vi verrà chiesto di fornire la password per la gestione domestica locale.


BitDefender
Inserire qui la password impostata quando è stata abilitata la Gestione domestica su questo PC.
Password
Non mostrare più questo messaggio durante questa sessione.
OK
Annulla

Inserire Password

2. Inserire la chiave con la quale vi volete registrare.


BitDefender
Registra BitDefender su questo PC - smandache
Digitare la chiave di licenza che si desidera utilizzare per registrare BitDefender in modo remoto.
Codice di licenza:
Esegui questa attività su tutti i computer
OK
Annulla

Registra tutti

3. Selezionare **OK**.

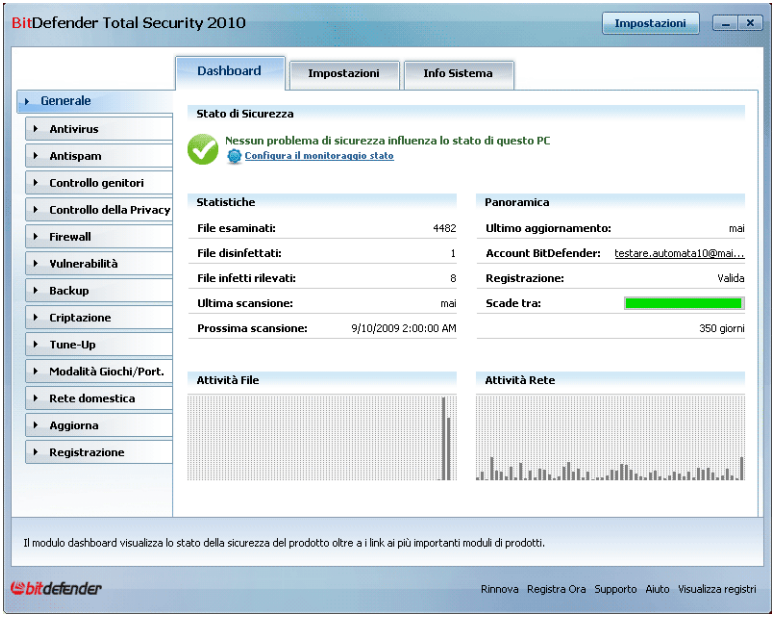
Modalità avanzata

17. Generale

Il modulo Generale fornisce informazioni sull'attività di BitDefender e sul sistema. Qui potete anche modificare il comportamento generale di BitDefender.

17.1. Dashboard

Per visualizzare le statistiche di attività del prodotto, lo stato di registrazione e se vi sono problemi che influiscono sul computer, andare a **Generale>Dashboard** in Modalità Avanzata.



Dashboard

La Dashboard ha diverse sezioni:

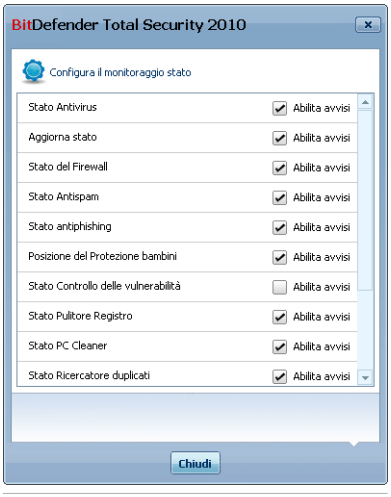
- **Stato Generale** - Informa in merito a qualsiasi problema che influenza la sicurezza del computer.
- **Statistiche** - Mostra importanti informazioni riguardanti l'attività di BitDefender.
- **Informazioni generali** - Mostra lo stato dell'aggiornamento, del vostro account, della registrazione ed informazioni sulla licenza.

- **Attività file** - Indica l'evoluzione del numero di elementi esaminati dall'Antimalware di BitDefender. L'altezza della barra indica l'intensità del traffico durante un intervallo di tempo.
- **Attività rete** - Indica l'evoluzione del traffico di rete filtrato dal Firewall BitDefender. L'altezza della barra indica l'intensità del traffico durante quell'intervallo di tempo.

17.1.1. Stato generale

Qui è possibile trovare il numero di problemi che mettono a rischio la sicurezza del computer. Per rimuovere tutte le minacce, fare clic su **Risolvi tutti i problemi**. Questo riavvia la procedura guidata Risolvi tutti i problemi.

Per configurare quali moduli verranno monitorati da Sicurezza totale BitDefender 2010, fare clic su **Configura monitoraggio stato**. Apparirà una nuova finestra:



Configura il monitoraggio stato

Se si desidera che BitDefender monitori un componente, selezionare la casella di controllo **Abilita allarmi** per il componente corrispondente. BitDefender può monitorare lo stato dei seguenti componenti di sicurezza:

- **Antivirus** - BitDefender monitora lo stato dei due componenti della funzione Antivirus: protezione in tempo reale e scansione su richiesta. I problemi più comuni riportati per questo componente vengono elencati nella seguente tabella.

Problema	Descrizione
La protezione in tempo reale è disabilitata	I file non vengono controllati quando viene effettuato l'accesso da parte vostra o da parte di un'applicazione in esecuzione sul sistema.
Non è mai stata eseguita la scansione del computer alla ricerca di malware	Non è mai stata compiuta una scansione del sistema su richiesta per controllare che i file contenuti sul computer siano esenti da malware.
L'ultima scansione di sistema avviata è stata annullata prima della sua conclusione	È stata avviata, ma non completata, una scansione completa del sistema.
L'Antivirus è in uno stato critico	La protezione in tempo reale del sistema è disabilitata e la scansione del sistema è ormai necessaria da lungo tempo.

- **Aggiornamento** - BitDefender controlla se le firme del malware sono aggiornate. I problemi più comuni riportati per questo componente vengono elencati nella seguente tabella.

Problema	Descrizione
L'Aggiornamento Automatico è disabilitato	Le firme del malware del prodotto BitDefender non vengono aggiornate automaticamente e regolarmente.
L'aggiornamento non è stato compiuto per x giorni	Le firme del malware del prodotto BitDefender sono obsolete.

- **Firewall** - BitDefender controlla lo stato della funzione Firewall. Se non è abilitata, verra riportato il problema **Firewall disabilitato**.
- **Antispam** - BitDefender controlla lo stato della funzione Antispam. Se non è abilitata, verra riportato il problema **Antispam disabilitato**.
- **Antiphishing** - BitDefender controlla lo stato della funzione di Antiphishing. Se non è abilitata per tutte le applicazioni supportate, verrà riportato il problema **Antiphishing disabilitato**.
- **Controllo Genitori** - BitDefender controlla lo stato della funzione Controllo Genitori. Se non è abilitata, verra riportato il problema **Controllo Genitori non configurato**.

- **Controllo Vulnerabilità** - BitDefender tiene traccia della funzione Controllo Vulnerabilità. Controllo Vulnerabilità comunica all'utente la necessità di installare aggiornamenti di Windows, aggiornamenti dell'applicazione e se è necessario rinforzare alcune password.

  I problemi più comuni riportati per questo componente vengono elencati nella seguente tabella.

Stato	Descrizione
Controllo Vulnerabilità è disabilitato	BitDefender non controlla potenziali vulnerabilità relative ad aggiornamenti di Windows mancanti, aggiornamenti delle applicazioni o password deboli.
Sono state individuate molteplici vulnerabilità	BitDefender ha trovato aggiornamenti di Windows/di applicazioni mancanti e/o password deboli.
Aggiornamenti critici Microsoft	Sono disponibili aggiornamenti di Windows critici, ma non sono stati installati.
Altri aggiornamenti Microsoft	Sono disponibili aggiornamenti di Windows non critici, ma non sono stati installati.
L'aggiornamento automatico di Windows è disabilitato	Gli aggiornamenti automatici di Windows non vengono automaticamente installati man mano che divengono disponibili.
`Applicazione` (obsoleta)	È disponibile una nuova versione dell'`Applicazione` ma non è stata installata.
`Utente` (Password Debole)	Individui malintenzionati possono individuare una password utente utilizzando software speciale.

- **Pulizia del Registro** - BitDefender tiene traccia del momento in cui è stato utilizzato per l'ultima volta questo strumento. Se l'esecuzione è stata rimandata troppo a lungo, verrà riportato il problema **Non è stata mai eseguita la Pulizia del Registro** / **La Pulizia del Registro non è stata eseguita per x giorni**.
- **Pulizia del PC** - BitDefender tiene traccia del momento in cui è stato utilizzato per l'ultima volta questo strumento. Se l'esecuzione è stata rimandata troppo a lungo, verrà riportato il problema **Non è stata mai eseguita la Pulizia del PC** / **La Pulizia del PC non è stata eseguita per x giorni**.
- **Ricercatore di Duplicati** - BitDefender tiene traccia del momento in cui è stato utilizzato per l'ultima volta questo strumento. Se l'esecuzione è stata rimandata troppo a lungo, verrà riportato il problema **Non è stato mai eseguito il Ricercatore di Duplicati** / **Il Ricercatore di Duplicati non è stato eseguito per x giorni**.

- **Deframmentazione Disco** - BitDefender tiene traccia del momento in cui è stato utilizzato per l'ultima volta questo strumento. Se l'esecuzione è stata rimandata troppo a lungo, verrà riportato il problema **Non è stata mai eseguita la Deframmentazione Disco** / **La Deframmentazione Disco non è stata eseguita per x giorni**.
- **Criptazione File** controlla lo stato del File Vault. Se non è abilitata, verrà riportato il problema **Criptazione File disabilitata**.
- **Backup Locale** controlla lo stato della funzione Backup Locale. Se non è stato effettuato un backup dei dati per un periodo di tempo eccessivo, verrà riportato il problema **Non è mai stato eseguito il backup locale dei dati** / **Il backup locale dei dati non è stato eseguito in x giorni**.

Importante
Per assicurarsi che il sistema sia completamente protetto abilitare il monitoraggio per tutti i componenti e risolvere tutti i problemi riportati.

17.1.2. Statistiche

Se volete dare un'occhiata all'attività di BitDefender, un buon posto per cominciare è la sezione Statistiche. Potete visualizzare i seguenti elementi:

Elemento	Descrizione
File esaminati	Indica il numero di file che sono stati esaminati alla ricerca di malware al momento dell'ultima scansione.
File disinfettati	Indica il numero dei file che sono stati disinfettati al momento della vostra ultima scansione.
File infettati rilevati	Indica il numero di file infetti che sono stati trovati nel sistema al momento dell'ultima scansione.
Ultima scansione del sistema	Indicata l'ultima scansione del computer. Se l'ultima scansione è stata eseguita più di una settimana fa, eseguire al più presto una nuova scansione. Per eseguire una scansione di tutto il computer, fare clic sulla scheda **Antivirus**, Scansione virus, ed eseguire una Scansione completa di sistema o una Scansione approfondita di sistema.
Prossima scansione	Indica la prossima volta in cui il computer verrà sottoposto a scansione.

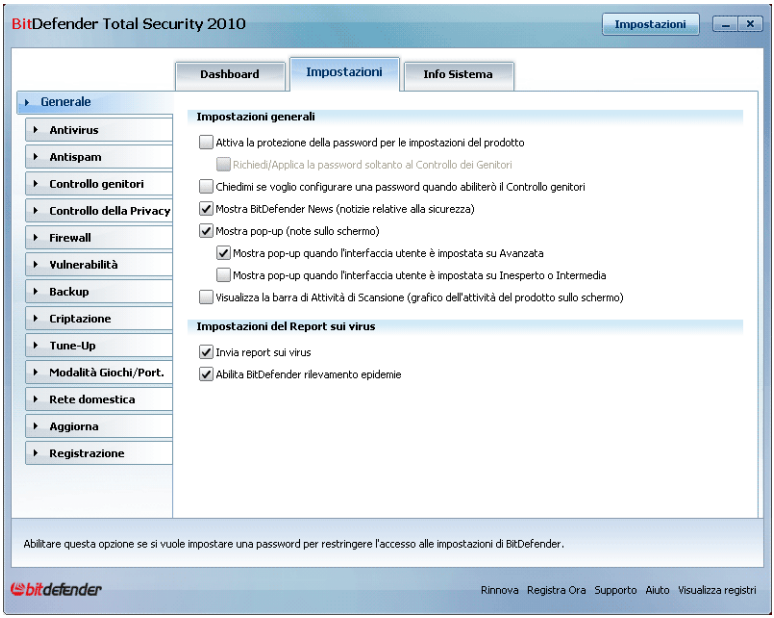
17.1.3. Panoramica

Qui è possibile vedere lo stato di aggiornamento, lo stato dell'account, le informazioni sulla registrazione e la licenza.

Elemento	Descrizione
Ultimo aggiornamento	Indicata quando è stato aggiornato per l'ultima volta il prodotto BitDefender. Eseguire aggiornamenti regolari per avere un sistema completamente protetto.
Account BitDefender	Indica l'indirizzo mail che potrete usare per accedere al vostro account on-line per recuperare la chiave di licenza BitDefender e beneficiare del supporto BitDefender e di altri servizi personalizzati È necessario creare un account BitDefender in modo da attivare il prodotto. Per ulteriori informazioni sull'account BitDefender, fare riferimento a «*Registrazione e Il mio Account*» (p. 52).
Registrazione	Indica il tipo e lo stato della vostra chiave di licenza. Per mantenere sicuro il vostro sistema dovete rinnovare o aggiornare BitDefender se la vostra chiave è scaduta.
Scade in	Indica il numero di giorni che mancano alla scadenza della chiave di licenza. Sa la chiave di licenza scade entro qualche giorno, registrare il prodotto con una nuova chiave di licenza. Per acquistare una chiave di licenza o rinnovare la licenza, fare clic sul link **Acquista/Rinnova**, situato in basso nella finestra.

17.2. Impostazioni

Per configurare e gestire le impostazioni generali di BitDefender andare su **Generale>Impostazioni** in Modalità Avanzata.


BitDefender Total Security 2010
Impostazioni
Dashboard
Impostazioni
Info Sistema
Generale
Antivirus
Antispam
Controllo genitori
Controllo della Privacy
Firewall
Vulnerabilità
Backup
Criptazione
Tune-Up
Modalità Giochi/Port.
Rete domestica
Aggiorna
Registrazione
Impostazioni generali
Attiva la protezione della password per le impostazioni del prodotto
Richiedi/Applica la password soltanto al Controllo dei Genitori
Chiedimi se voglio configurare una password quando abiliterò il Controllo genitori
Mostra BitDefender News (notizie relative alla sicurezza)
Mostra pop-up (note sullo schermo)
Mostra pop-up quando l'interfaccia utente è impostata su Avanzata
Mostra pop-up quando l'interfaccia utente è impostata su Inesperto o Intermedia
Visualizza la barra di Attività di Scansione (grafico dell'attività del prodotto sullo schermo)
Impostazioni del Report sui virus
Invia report sui virus
Abilita BitDefender rilevamento epidemie
Abilitare questa opzione se si vuole impostare una password per restringere l'accesso alle impostazioni di BitDefender.
bitdefender
Rinnova Registra Ora Supporto Aiuto Visualizza registri

Impostazioni generali

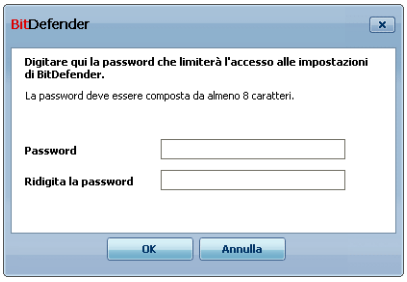
Da qui è possibile impostare il comportamento generale di BitDefender. BitDefender è caricato automaticamente all'avvio di Windows e successivamente minimizzato nella barra strumenti.

17.2.1. Impostazioni generali

- **Abilita la protezione password per le impostazioni del prodotto** - consente l'impostazione di una password per proteggere la configurazione di BitDefender.

  Nota
  Se non siete l'unica persona ad utilizzare questo computer, consigliamo di proteggere le vostre Impostazioni BitDefender con una password.

  Selezionando questa opzione, apparirà la seguente finestra:



Conferma password

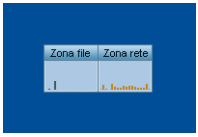
Digitare la password nel campo **Password**, quindi re-inserirla nel campo **Ridigitare password** e selezionare **OK**.

Una volta che avete impostato la password, vi verrà chiesta ogni volta che vorrete cambiare le impostazioni di BitDefender. Gli altri amministratori del sistema (se ci sono) dovranno anche loro fornire questa password per cambiare le impostazioni di BitDefender.

Se volete che vi venga richiesta la password solo quando configurate il Controllo dei Genitori, dovrete selezionare anche **Chiedere/Applicare password al Controllo dei Genitori**. Inoltre, se una password è stata impostata per il Controllo dei Genitori e deselezionate questa opzione, la rispettiva password verrà chiesta per configurare qualsiasi opzione di BitDefender.

Importante
Se si dimentica la password, si deve riparare il prodotto per modificare la configurazione BitDefender.

- **Chiedimi se voglio configurare una password per l'abilitazione del Controllo dei Genitori** - vi chiede di configurare una password quando desiderate abilitare il Controllo dei Genitori e non è stata impostata nessuna. Impostando una password, impedirete ad altri utenti con diritti di amministratore di modificare le impostazioni del Controllo dei Genitori che avete configurato per un utente specifico.
- **Ricezione notifiche di sicurezza** - riceve di volta in volta, dai server BitDefender, segnalazioni di sicurezza relative alla diffusione di nuovi virus.
- **Mostra pop-ups (attiva la schermata delle note)** - mostra finestre a tendina relative allo stato del prodotto. È possibile configurare BitDefender affinché visualizzi pop-up solo quando l'interfaccia è nella Modalità Inesperto / Intermedia o nella Modalità Avanzata.
- **Vusalizza barra di attività della scansione (grafico dell'attività del prodotto a schermo)** - mostra la barra delle Attività della Scansione ogni volta che si accede a Windows. Deselezionare la casella se non volete che la barra delle Attività di Scansione venga mostrata ancora.



Barra di Attività della Scansione

Nota

Questa opzione può essere configurata solo per l'account di Windows in uso. La barra dell'attività di scansione è disponibile solo quando l'interfaccia è in Modalità Avanzata.

17.2.2. Impostazioni del Report sui virus

- **Invia rapporti dei virus** - invia ai Laboratori BitDefender i rapporti relativi ai virus identificati sul vostro computer. Questo ci aiuta a tracciare la diffusione dei virus.

  I rapporti non contengono dati confidenziali, come il vostro nome, l'indirizzo IP o altri, e non verranno utilizzati per scopi commerciali. Le informazioni fornite conterranno solo il nome del virus e verranno utilizzate unicamente per creare rapporti statistici.

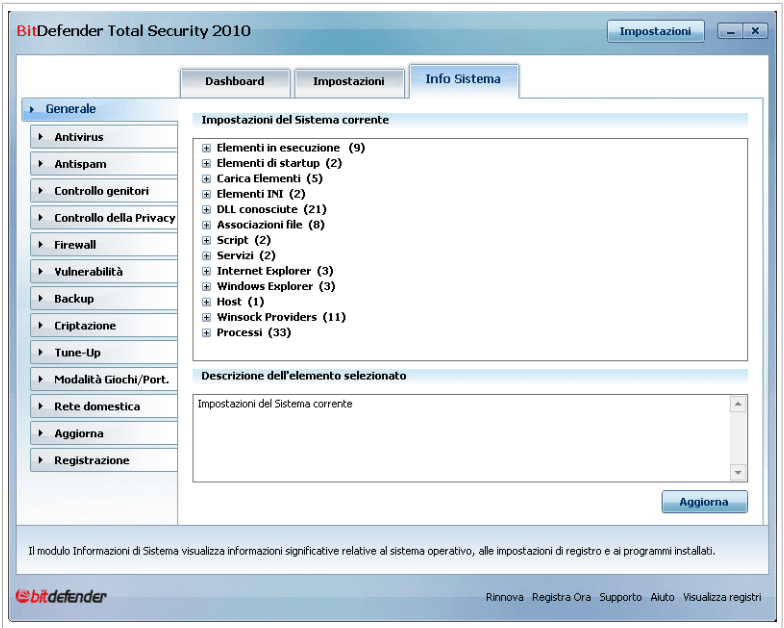
- **Attivare Outbreak Detection BitDefender** - invia ai Laboratori BitDefender i report relativi al potenziale scoppio di un virus.

  I report non contengono dati confidenziali, come il vostro nome, l'indirizzo IP o altri, e non verranno utilizzati per scopi commerciali. Le informazioni fornite conterranno esclusivamente il nome del virus e verranno utilizzate per creare report statistici.

17.3. Sistema Informazione

BitDefender vi permette di visualizzare, da una singola ubicazione, tutta la configurazione del sistema e le applicazioni che verranno eseguite all'avvio. In questo modo potrete monitorare l'attività del sistema e delle applicazioni installate così come identificare possibili infezioni del sistema.

Per ottenere informazioni sul sistema, cliccare su **Generale>Informazioni di Sistema** in Modalità Avanzata.



Sistema Informazione

La lista contiene tutti gli elementi caricati quando si avvia il sistema oltre agli elementi caricati da varie applicazioni.

Tre pulsanti sono disponibili:

- **Ripristinare** - Cambia l'associazione di un file corrente a quella di default. Disponibile solo per le impostazioni delle **Associazioni File**!
- **Vai a** - apri una finestra dove l'elemento selezionato è situato (la **Registrazione** ad esempio).

  Nota
  A seconda dell'elemento selezionato, il pulsante **Vai a** potrebbe non apparire.

- **Aggiorna** - riapri la sezione del **Sistema Informazione** section.

18. Antivirus

BitDefender protegge il vostro computer da ogni tipo di minaccia malware (virus, troiani, spyware, rootkit ed altro). La protezione che BitDefender vi offre è divisa in due categorie:

- Protezione in tempo reale - previene l'ingresso di nuove minacce malware nel vostro sistema. BitDefender esaminerà, ad esempio, un documento word quando verrà aperto, ed una mail quando verrà ricevuta.

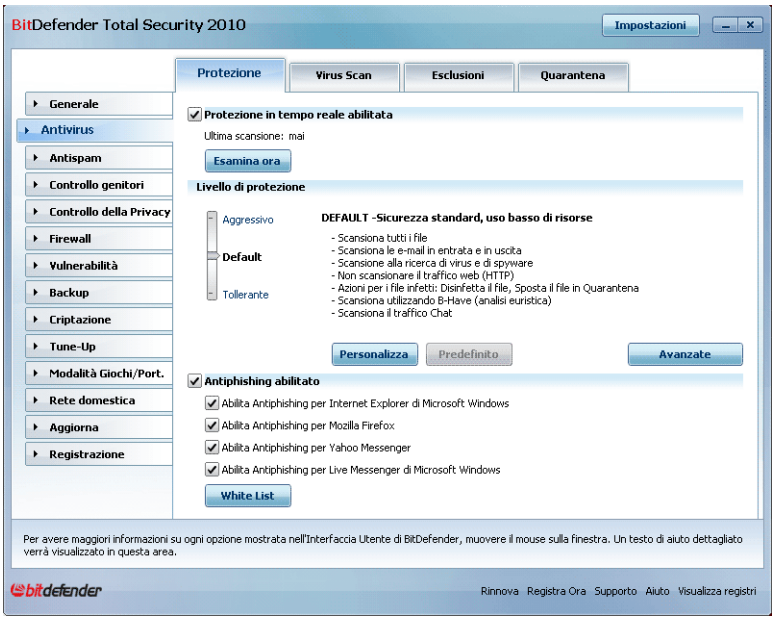
  Nota
  La protezione in tempo reale si riferisce anche alla scansione "all'accesso" - i file vengono esaminati nel momento in cui gli utenti vi accedono.

- Scansione a richiesta - permette di rilevare e di rimuovere malware già residente nel vostro sistema. Si tratta della classica scansione dei virus avviata dall'utente – si sceglie quale drive, cartella o file BitDefender deve esaminare e BitDefender li esamina – a richiesta. I processi della scansione vi permettono di creare routine di scansione personalizzate e la loro esecuzione può essere programmata con una cadenza regolare.

18.1. Protezione in tempo reale

BitDefender fornisce una continua protezione in tempo reale contro un ampio spettro di minacce malware mediante la scansione di tutti i file nei quali si è effettuato l'accesso, le mail e le comunicazioni tramite applicazioni Software di Messaggistica Istantanea (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). BitDefender Antiphishing vi impedisce di svelare informazioni personali mentre navigate su internet avvertendovi delle potenziali pagine web con phishing.

Per configurare la protezione in tempo reale e BitDefender Antiphishing, fare clic su **Antivirus>Shield** in Modalità Avanzata.



Protezione in tempo reale

Potete vedere se la Protezione in tempo reale è abilitata o disabilitata. Se volete cambiare lo stato della Protezione in tempo reale, selezionare o deselezionare la casella corrispondente.

Importante
Per impedire ai virus di infettare il vostro computer, tenere abilitato il **Virus Shield**.

Per avviare una scansione del sistema, fare clic su **Scansiona Ora**.

18.1.1. Configurazione del Livello di Protezione

Potete scegliere il livello di protezione che meglio si adatta alle vostre necessità di sicurezza. Trascinate il pulsante sulla barra per impostare il livello di protezione appropriato.

Ci sono 3 livelli di protezione:

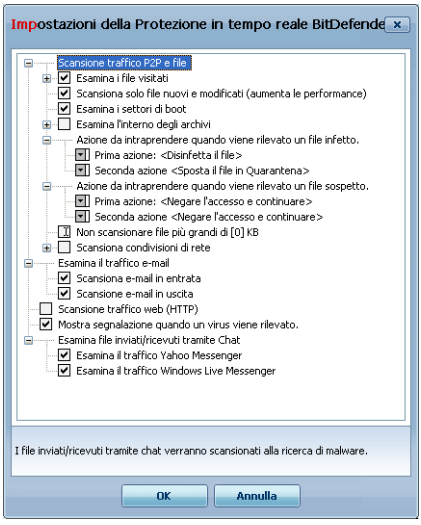
Livello di protezione	Descrizione
Permissiva	Copre le necessità di sicurezza di base. Il livello di consumo delle risorse è molto basso. Solo i programmi e i messaggi di posta in arrivo sono scansionati solo alla ricerca di virus. Oltre alla classica scansione basata sulla firma, è utilizzata anche l'analisi euristica. Le azioni prese sui file infetti sono le seguenti: pulisci file/sposta in quarantena.
Default	Offre una sicureza standard. Il livello di consumo delle risorse è basso. Tutti i file e i messaggi di posta in arrivo ed in uscita sono esaminati alla ricerca di virus e spyware. Oltre alla classica scansione basata sull'impronta, è utilizzata anche l'analisi euristica. Le azioni prese sui file infetti sono le seguenti: pulisci file/sposta in quarantena.
Aggressiva	Offre una sicurezza alta. Il livello di consumo delle risorse è moderato. Tutti i file, e i messaggi e-mail in entrata ed in uscita ed il traffico web sono esaminati alla ricerca di virus e spyware. Oltre alla classica scansione basata sull'impronta, è utilizzata anche l'analisi euristica. Le azioni prese sui file infetti sono le seguenti: pulisci file/sposta in quarantena.

Per applicare le impostazioni di protezione in tempo reale di default cliccare su **Livello di Default**.

18.1.2. Livello di Protezione Personalizzato

Gli utenti esperti possono trarre vantaggio dalle possibilità di impostazione della scansione BitDefender. Infatti la scansione può essere impostata in modo di esaminare solo delle specifiche estensioni, di cercare delle particolare minacce malware, o di non esaminare gli archivi. Questo può ridurre di molto i tempi di scansione ed incrementare la reattività del vostro computer durante una scansione.

Potete personalizzare la **Real-time protection** cliccando **Custom level**. Apparirà la seguente finestra:



Impostazioni Virus Shield

Le opzioni di scansione sono organizzate come menu espandibili, molto simili a quelli di esplorazione di Windows. Selezionare la casella con "+" per aprire un'opzione oppure la casella con "-" per chiudere un'opzione.

Nota
Si può vedere come alcune opzioni di scansione, nonostante appaia il segno "+", non possano essere aperte. Il motivo è che queste opzioni non sono ancora state selezionate. Si può notare che sarà possibile aprirle una volta selezionate.

- **Scansione dei file acceduti e dei transferimenti P2P** - esamina i file acceduti e le comunicazioni tramite applicazioni Software di Messaggistica Istantanea (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Successivamente selezionare il tipo di file che si desidera esaminare.

Opzione		Descrizione
Esamina i files acceduti	**Tutti i file**	Verranno esaminati tutti i file acceduti, indipendentemente dalla loro tipologia.
	Scansiona solo applicazioni	Verranno esaminati solo i file di programma. Questo significa solo i file con le seguenti estensioni: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`;

Opzione		Descrizione
		.doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml e .nws.
	Estensioni definite dall'utente	Verranno esaminati soltanto i file con le estensioni specificate dall'utente. Le varie estensioni devono essere separate da ";".
	Scansione per riskware	Esamina alla ricerca di riskware. Questi file verranno trattati come file infetti. Software che includono componenti adware potrebbero bloccarsi se questa opzione è attiva. Seleziona **Ignora dialer e applicazioni durante la scansione** e/o **Ignora keylogger durante la scansione** se si desidera escludere questi tipi di file dalla scansione.
Scansiona solo i file nuovi e modificati		Scansiona solo i file che non sono stati scansionati in precedenza o che sono stati cambiati dall'ultima scansione. Selezionando questa opzione, è possibile migliorare di molto la risposta generale del sistema con un minimo compromesso per la sicurezza.
Esamina settore di boot		Per esaminare i settori di avvio del sistema.
Esamina gli archivi		Verranno esaminati anche gli archivi acceduti. Con questa opzione abilitata, il computer sarà più lento. È possibile impostare la dimensione massima di archivi da scansionare (in kilobyte, digitare 0 se si vogliono scansionare tutti gli archivi) e la profondità massima di archivi da scansionare.
Prima azione		Seleziona dal menù delle opzioni la prima azione da intraprendere su files infetti o sospetti:
	Rifiuta l'accesso e continua	Nel caso di individuazione di un file infetto, l'accesso al file verrà negato.

Opzione		Descrizione
	Disinfetta i file	Rimuove il codice malware da file infetti.
	Cancella file	Cancella immediatamente i file infetti, senza alcun avviso.
	Muovi file nella Quarantena	Sposta i file infetti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.
Seconda azione		Seleziona la seconda azione dalle opzioni da intraprendere sui files infetti, nel caso in cui la prima fallisse.
	Rifiuta l'accesso e continua	Nel caso di individuazione di un file infetto, l'accesso al file verrà negato.
	Cancella file	Cancella immediatamente i file infetti, senza alcun avviso.
	Muovi file nella Quarantena	Sposta i file infetti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.
Non scansionare i file più grandi di [x] Kb		Digitare la dimensione massima dei files da esaminare. Se la dimensione è pari a 0 Kb, tutti i files verranno esaminati.
Scansionare condivisioni di rete	**Tutti i file**	Verranno scansionati tutti i file acceduti dalla rete, indipendentemente dalla loro tipologia.
	Scansiona solo applicazioni	Verranno esaminati solo i file di programma. Questo significa solo i file con le seguenti estensioni: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml` e `.nws`.
	Estensioni definite dall'utente	Verranno esaminati soltanto i file con le estensioni specificate dall'utente. Le varie estensioni devono essere separate da ";".

- **Esamina il traffico e-mail** - tutti i messaggi e-mail vengono esaminati.

  Sono disponibili le seguenti opzioni:

Opzione	Descrizione
Esamina le e-mail in ingresso	Tutte le e-mail in ingresso vengono esaminate.
Esamina le e-mail in uscita	Tutte le e-mail in uscita vengono esaminate.

- **Scansiona il traffico web (HTTP)** - tutto il traffico http viene scansionato.
- **Mostra avviso, se viene rilevato un virus** - verrà visualizzata una finestra di avviso quando verrà rilevato un virus in un file o in un messaggio e-mail.

  In presenza di un virus, si aprirà una finestra contenente il nome del virus, e che permetterà di selezionare un azione sul file infetto adottato dal BitDefender, e un link al sito BitDefender dove è possibile trovare ulteriori informazioni al riguardo. Per una e-mail infetta, la finestra di allerta contiene anche informazioni sul mittente e il destinatario.

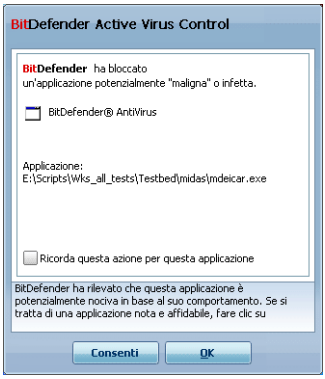
  In caso che un file sospetto è scansionati, puoi lanciare un wizard dalla finestra di allerta che ti aiuterà a spedire il file ai Laboratori BitDefender per una ulteriore analisi. È possibile scrivere dalla tua e-mail per ricevere informazioni su questo report.
- **Esamina file ricevuti/inviati tramite IM.** Per esaminare i file che ricevete o inviate usando Yahoo Messenger o Windows Live Messenger, selezionare la casella corrispondente.

Selezionare **OK** per salvare le modifiche e chiudere la finestra.

18.1.3. Configurazione Active Virus Control

BitDefender Active Virus Control fornisce un livello di protezione contro nuove minacce le cui firme non sono ancora state rilasciate. Analizza e monitora costantemente il comportamento delle applicazione in esecuzione sul vostro computer e vi avverte se una di queste ha un comportamento sospetto.

AVC può essere configurato per avvisare e richiedere un'azione dell'utente ogni volta che un'applicazione prova a compiere un'azione potenzialmente nociva.


BitDefender Active Virus Control
BitDefender ha bloccato
un'applicazione potenzialmente "maligna" o infetta.
BitDefender® AntiVirus
Applicazione:
E:\Scripts\Wks_all_tests\Testbed\midas\mdeicar.exe
Ricorda questa azione per questa applicazione
BitDefender ha rilevato che questa applicazione è potenzialmente nociva in base al suo comportamento. Se si tratta di una applicazione nota e affidabile, fare clic su
Consenti
OK

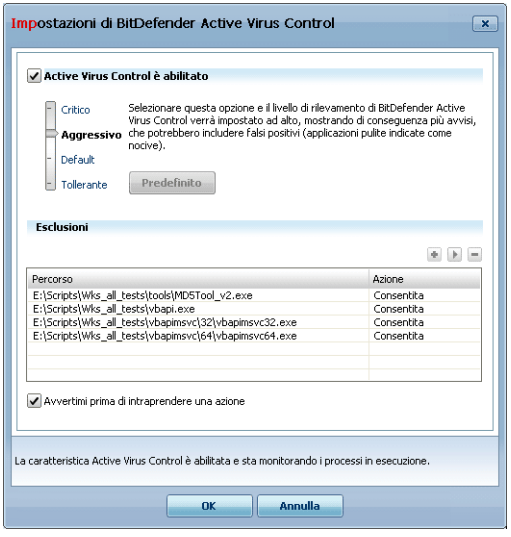
Avviso Active Virus Control

Se conoscete e vi fidate dell'applicazione rilevata, cliccare su **Consentire**.

Se volete chiudere immediatamente l'applicazione, cliccare su **OK**.

Selezionare la casella di controllo **Ricorda questa azione per questa applicazione** prima di eseguire la propria scelta e BitDefender eseguirà la stessa azione per l'applicazione rilevata in futuro. La regola creata viene elencata nella finestra di configurazione Active Virus Control,

Per configurare Active Virus Control, fare clic su **Impostazioni Avanzate**.



Impostazioni Active Virus Control

Selezionare la casella di controllo corrispondente per abilitare Active Virus Control.

Importante
Mantenere Active Virus Control abilitato per essere protetti contro virus sconosciuti.

Se si desidera ricevere avvisi e richieste di azione da parte di Active Virus Control quando una applicazione tenta di eseguire una possibile azione nociva, selezionare la casella di controllo **Chiedi cosa fare**.

Configurazione del Livello di Protezione

Il livello di protezione di AVC cambia automaticamente quando viene impostato un nuovo livello di protezione in tempo reale. Se non siete soddisfatti delle impostazioni di default, potete configurare manualmente il livello di protezione.

Nota

Tenere presente che se viene cambiato il livello corrente di protezione in tempo reale, il livello di protezione di AVC cambierà di conseguenza. Se si imposta la protezione in tempo reale su **Permissiva**, Active Virus Control viene disabilitato automaticamente. In questo caso è possibile abilitarlo manualmente quando si desidera usarlo.

Trascinate il pulsante scorrevole lungo la barra per impostare il livello di protezione che meglio si adatta alle vostre esigenze di sicurezza.

Livello di protezione	Descrizione
Critico	Controllo rigido di tutte le applicazioni alla ricerca di possibili azioni nocive.
Default	Il tasso di rilevamento è elevato e sono possibili dei falsi positivi.
Medio	Controllo dell'applicazione moderato, sono ancora possibili dei falsi positivi.
Permissiva	I tassi di rilevamento sono bassi e non vi sono falsi positivi.

Gestione delle Applicazioni Affidabili / Non affidabili

È possibile aggiungere applicazioni note e affidabili all'elenco di applicazioni affidabili. Queste applicazioni non verranno più controllate da BitDefender Active Virus Control e verrà concesso loro accesso automaticamente.

Le applicazioni per cui sono state create delle regole vengono elencate nella tabella alla voce **Esclusioni**. Per ciascuna regola viene visualizzato il percorso dell'applicazione e l'azione impostata (Permessa o Bloccata).

Per modificare l'azione per un'applicazione fare clic sull'azione attuale e selezionare la nuova azione dal menu.

Per gestire l'elenco utilizzare i pulsanti posizionati al di sotto della tabella:

- **Aggiungi** - per aggiungere una nuova applicazione alla lista.
- **Rimuovi** - per rimuovere una applicazione dalla lista.

Modifica - modifica una regola di applicazione.

18.1.4. Disattivazione Protezione in Tempo Reale

Se volete disattivare la protezione in tempo reale, apparirà la seguente finestra di avviso: Dovrete confermare la vostra scelta selezionando dal menu, per quanto tempo volete disattivare la protezione in tempo reale. Potete disattivarla durante 5, 15 o 30 minuti, un'ora, permanentemente o fino al riavvio del sistema.

Avvertimento

Questa è una questione di sicurezza critica. Vi consigliamo di disattivare la protezione in tempo reale per il minimo tempo possibile. Se la protezione in tempo reale non è attiva, non sarete protetti dalle minacce malware.

18.1.5. Configurazione della Protezione Antiphishing

BitDefender fornisce protezione antiphishing in tempo reale per:

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger
- Windows Live (MSN) Messenger

Potete scegliere di disabilitare la protezione antiphishing completamente o solo per applicazioni specifiche.

Potete cliccare su **White List** per configurare e gestire un elenco di pagine web che non devono essere esaminate dai motori Antiphishing BitDefender.

BitDefender Total Security 2010
White List
Questo è l'elenco di URL che non saranno filtrati dai motori Antiphishing di BitDefender.
Le URL inserite nell'elenco non verranno assolutamente controllate dai motori antiphishing di BitDefender. Nessuna informazione verrà visualizzata su alcuna minaccia esistente in queste pagine.
Aggiungi URL:
Aggiungi
Sito web
www.google.ro
Rimuovi
Fare clic qui per aggiungere l'URL alla White List Antiphishing.
Chiudi
Salva

White List Antiphishing

Potete vedere i siti web che BitDefender non controlla attualmente per contenuti phishing.

Per aggiungere un sito alla White List, inserire il suo indirizzo url nel campo corrispondente **Nuovo indirizzo** quindi cliccare **Aggiungi**. La white list dovrebbe contenere solo siti web di cui vi fidate completamente. Ad esempio, aggiungere siti web dove fate di solito i vostri acquisti online.

Nota

Potete aggiungere facilmente dei siti web alla White List utilizzando la barra degli strumenti Antiphishing BitDefender integrata nel vostro browser. Per ulteriori informazioni, fare riferimento a «*Integrazione nei Web Browser*» (p. 360).

Per rimuovere un sito web dalla white list, fare clic sul pulsante corrispondente **Rimuovi**.

Fare clic su **Salva** per salvare le modifiche e chiudere la finestra.

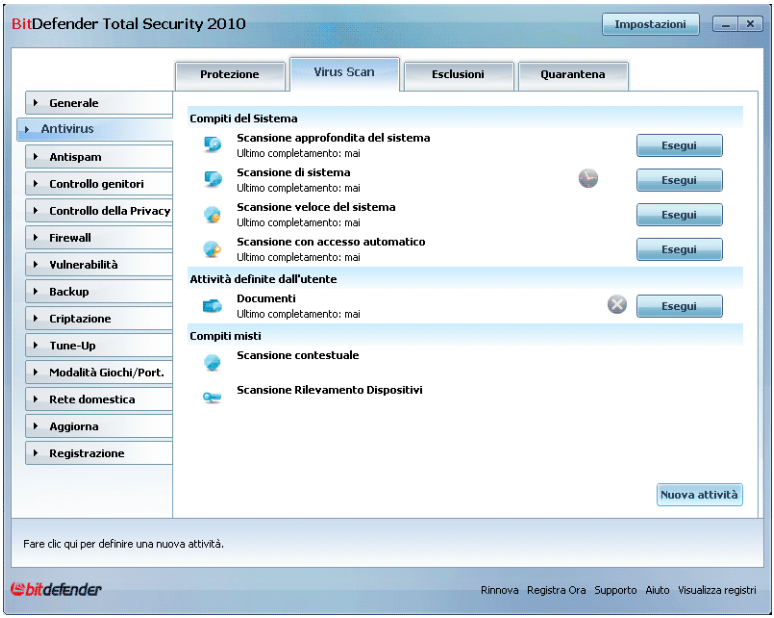
18.2. Scansione a richiesta

L'obiettivo principale di BitDefender è di mantenere il vostro computer privo di virus. Ciò avviene principalmente tenendo lontani i nuovi virus dal vostro computer ed

esaminando i vostri messaggi e-mail e qualsiasi nuovo file scaricato o copiato sul vostro sistema.

Esiste il rischio che un virus sia già contenuto nel vostro sistema, addirittura prima dell'installazione di BitDefender. Questo è il motivo per cui suggeriamo di effettuare una scansione sul vostro computer alla ricerca di virus residenti dopo aver installato BitDefender. inoltre di effettuare frequentemente una scansione del vostro computer alla ricerca di virus.

Per configurare ed avviare la scansione a richiesta, fare clic su **Antivirus>Virus Scan** nella Modalità Avanzata.



Impostazioni della Scansione

La scansione a richiesta si basa sulle impostazioni della scansione. Le impostazioni della scansione specificano le opzioni della scasione e gli oggetti da esaminare. Potete esaminare il vostro computer in qualsiasi momento, eseguendo le funzioni predefinite oppure le vostre (definite dall'utente). Potete anche programmarle affinchè vengano eseguite con cadenza regolare oppure quando il sistema è inattivo in modo da non interferire con il vostro lavoro.

18.2.1. Impostazioni della Scansione

BitDefender ha tante funzioni, create per default, che coprono i problemi di sicurezza comuni. Voi potete anche creare le vostre funzioni di scansione personalizzate.

Vi sono tre categorie di compiti di scansione:

- **Funzioni di Sistema** - contiene la lista delle funzioni di sistema di default. Sono disponibili i compiti seguenti:

Funzione di Default	Descrizione
Scansione del Sistema approfondita	Esamina l'intero sistema. Nella configurazione predefinita, esegue la scansione per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.
Scansione sistema	Esamina l'intero sistema, esclusi gli archivi. Nella configurazione di default la scansione ricerca tutti i tipi di malware ad eccezione dei rootkit.
Scansione Veloce del Sistema	Scansiona le cartelle `Windows` e `Program Files`. Nella configurazione predefinita, esamina per cercare tutti i tipi di malware, esclusi i rootkit, ma non esamina la memoria, il registro nè i cookies.
Scansione accesso automatico	Esamina gli elementi che vengono eseguiti quando un utente accede a Windows. Di default, la scansione autologon è disabilitata Se si vuole utilizzare questa attività, fare clic con il pulsante destro e selezionare **Programma** e impostare l'attività per l'esecuzione **all'avvio del sistema**. Specifica dopo quanto tempo dal suo inizio, il compito deve essere fermato.

Nota

Poiché le funzioni **Scansione approfondita del sistema** e **Scansione completa del sistema** analizzano l'intero sistema, la scansione può richiedere un po' di tempo. Quindi consigliamo di eseguire questi compiti con priorità bassa o, meglio, quando il sistema è inattivo.

- **Impostazione Utente** - contiene le impostazioni definite dall'utente.

  Viene fornita una funzione chiamata `My Documents`. Utilizzare questa funzione per esaminare delle cartelle importanti dell'utente corrente: `My Documents`, `Desktop` e `StartUp`. Questo garantirà la sicurezza dei vostri documenti, uno spazio di lavoro sicuro ed applicazioni pulite al avvio.

- **Compiti misti** - contiene un elenco di compiti di scansione misti. Questi compiti di scansione si riferiscono a tipi di scansione alternativi che non possono essere eseguiti da questa finestra. Potete solo modificare le loro impostazioni o vedere i report delle scansioni.

Ogni attività ha una finestra **Proprietà** che ne permette la configurazione e la visualizzazione dei registri di scansione. Per aprire tale finestra fare doppio clic sul pulsante **Proprietà** prima del nome dell'attività. Per ulteriori informazioni fare riferimento a «*Configurare un Compito di Scansione*» (p. 176).

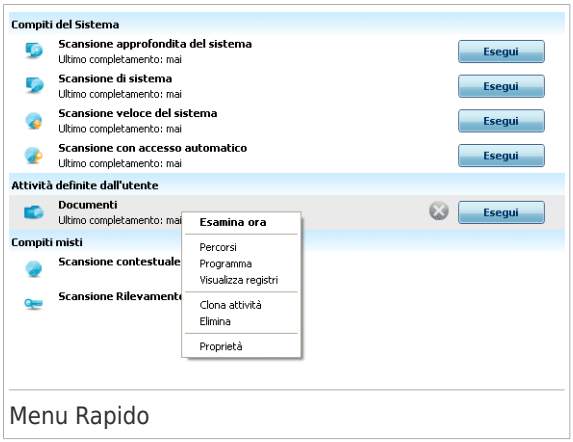
Per eseguire una scansione di sistema o definita dall'utente, fare clic sul pulsante **Esegui Attività** corrispondente. La Procedura guidata scansione antivirus apparirà e guiderà attraverso il processo di scansione.

Quando un'attività è programmata per essere eseguita automaticamente, in un momento successivo o regolarmente, viene visualizzato il pulsante **Programma** a destra dell'attività. Fare clic su questo pulsante per aprire la finestra **Proprietà**, scheda Programmazione, dove è possibile vedere e modificare il programma dell'attività.

Se non è più necessaria un'attività di scansione creata (definita dall'utente), è possibile cancellare facendo clic sul pulsante **Elimina**, a destra dell'attività. Non è possibile rimuovere attività varie o di sistema.

18.2.2. Utilizzo del Menu Rapido

Un menu rapido è disponibile per ciascun compito. Cliccare col pulsante destro del mouse sul compito selezionato per aprirlo.



Menu Rapido

Per le attività di sistema e definite dall'utente sono disponibili i seguenti comandi nel menu di scelta rapida:

- **Scan Now** - esegue la funzione selezionata, avviando immediatamente una scansione.
- **Target di Scansione** - apre la sezione Percorso Scansione nella finestra delle **Proprietà**, dove potete cambiare il target di scansione per i compiti selezionati.

Nota
Nel caso di funzioni del sistema, questa opzione viene sostituita da **Mostrare percorsi delle scansioni**, dato che è possibile vedere solo il loro target di scansione.

- **Schedule** - apre la**Finestra proprietà** Programma tab, dove puoi programmare i compiti selezionati.
- **Visualizza registri** - apre la finestra **Proprietà**, scheda Registri dove è possibile vedere i report generati dopo che l'attività selezionata è stata eseguita.
- **Attività di clonazione** - duplica l'attività selezionata. Ciò è utile quando si creano nuovi compiti, in quanto potete modificare le impostazioni del compito duplicato.
- **Cancella** - cancella i compiti selezionati.

Nota
Non disponibile per compiti di sistema. Non potete rimuovere un compito di sistema.

- **Proprietà** - apre la finestra **Proprietà**, scheda Panoramica, dove è possibile cambiare le impostazioni dell'attività selezionata.

Data la particolare natura della categoria **Attività varie** solo le opzioni **Visualizza registri** e **Proprietà** sono disponibili in questo caso.

18.2.3. Creazione delle Funzioni di Scansione

Per creare un compito di scansione, utilizzare uno di questi metodi:

- Duplica una attività esistente, rinominala ed apporta le modifiche necessarie nella finestra delle Proprietà.
- Cliccare **Nuovo Compito** per creare un nuovo compito e configurarlo.

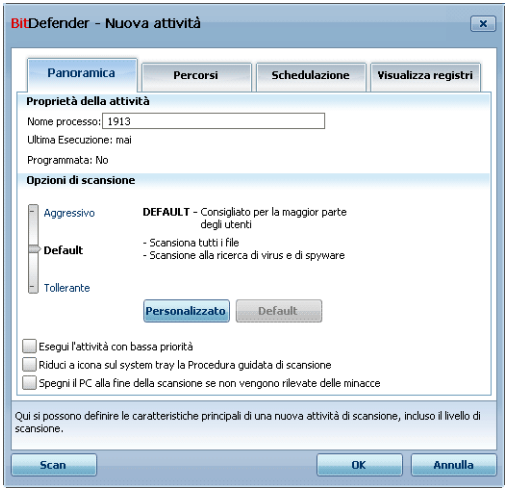
18.2.4. Configurare un Compito di Scansione

Ogni compito di scansione ha la sua propria finestra delle **Proprietà**, dove potete configurare le opzioni di scansione, impostare il target della scansione, programmare il compito o vedere i report. Per aprire questa finestra fare clic sul pulsante **Proprietà** alla sinistra dell'attività (o fare clic con il pulsante destro sull'attività e poi fare clic su **Proprietà**). E' anche possibile fare doppio clic sull'attività.

Nota
Per ulteriori informazioni sulla visualizzazione dei registri e sulla funzione **Visualizza Registri**, fare riferimento a «*Visualizzazione dei Registri di Scansione*» (p. 196).

Configurazione delle Impostazioni di Scansione

Per configurare le opzioni di scansione di un'attività specifica, fare clic con il pulsante destro e selezionare**Proprietà**. Apparirà la finestra seguente:


BitDefender - Nuova attività
Panoramica
Percorsi
Schedulazione
Visualizza registri
Proprietà della attività
Nome processo: 1913
Ultima Esecuzione: mai
Programmata: No
Opzioni di scansione
Aggressivo
Default
Tollerante
DEFAULT - Consigliato per la maggior parte degli utenti
- Scansiona tutti i file
- Scansione alla ricerca di virus e di spyware
Personalizzato
Default
Esegui l'attività con bassa priorità
Riduci a icona sul system tray la Procedura guidata di scansione
Spegni il PC alla fine della scansione se non vengono rilevate delle minacce
Qui si possono definire le caratteristiche principali di una nuova attività di scansione, incluso il livello di scansione.
Scan
OK
Annulla

Panoramica

Qui potete vedere le informazioni sul compito (nome, ultima esecuzione e stato della programmazione) ed impostare le impostazioni di scansione.

Scelta del Livello di Scansione

Potete facilmente configurare le impostazioni di scansione scegliendo il livello di scansione. Trascinare l'indicatore sulla barra per impostare l'appropriato livello di scansione.

Ci sono 3 livelli di scansione:

Livello di protezione	Descrizione
Permissiva	Offre un'efficienza di rilevamento ragionevole. Il livello di consumo delle risorse è basso.

Livello di protezione	Descrizione
	Vengono esaminati alla ricerca di virus solo i programmi. Oltre alla classica scansione basata sulla firma, è utilizzata anche l'analisi euristica.
Medio	Offre una buona efficienza di rilevamento. Il livello di consumo delle risorse è moderato. Tutti i file vengono esaminati alla ricerca di virus e spyware. Oltre alla classica scansione basata sulle impronte, è utilizzata anche l'analisi euristica.
Aggressiva	Offre un'alta efficienza di rilevamento. Il livello di consumo di risorse è alto. Tutti i file e gli archivi vengono esaminati alla ricerca di virus e spyware. Oltre alla classica scansione basata sulle impronte, è utilizzata anche l'analisi euristica.

È anche disponibile una serie di opzioni generali per il processo di scansione:

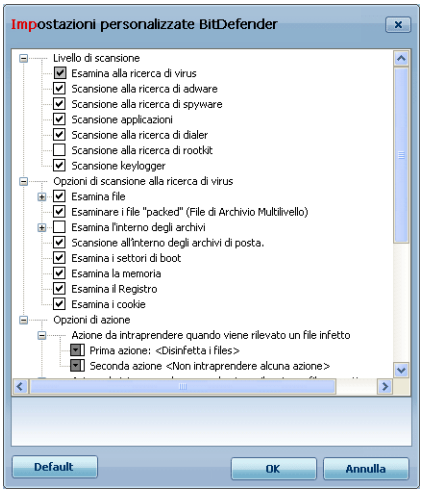
- **Esegui il task di scansione con Bassa Priorità.** Riduce la priorità del processo di scansione. Permetterai ad altri programmi di essere più veloci ed incrementerai il tempo necessario per finire il processo di scansione.
- **Minimizza la finestra di scansione nel systray.** Riduce a icona la finestra di scansione sulla barra degli strumenti. Eseguire un doppio clic sull'icona di BitDefender per riaprirla.
- **Spegnere il computer quando la scansione sia completata e non siano state rilevate delle minacce**

Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scansione**.

Personalizzazione del Livello di Scansione

Gli utenti esperti possono trarre vantaggio dalle possibilità di impostazione della scansione BitDefender. Infatti la scansione può essere impostata in modo di esaminare solo delle specifiche estensioni, di cercare delle particolare minacce malware, o di non esaminare gli archivi. Questo può ridurre di molto i tempi di scansione ed incrementare la reattività del vostro computer durante una scansione.

Cliccare su **Personalizza** per impostare le vostre opzioni di scansione. Si aprirà una nuova finestra.



Impostazioni di Scansione

Le opzioni di scansione sono organizzate come menu espandibili, molto simili a quelli di esplorazione di Windows. Selezionare la casella con "+" per aprire un'opzione oppure la casella con "-" per chiudere un'opzione.

Le opzioni di scansione sono raggruppate in 3 categorie:

- **Livello di Scansione.** Specificare il tipo di malware che volete che Bit Defender analizzi, selezionando le opzioni appropriate dalla categoria **Livello di scansione**.

Opzione	Descrizione
Scansione Virus	Esamina per virus conosciuti. BitDefender rileva anche virus incompleti, rimuovendo ogni possibile minaccia che possa colpire la sicurezza del vostro sistema.
Scansione adware	Esegue la scansione per minacce adware. Questi file verranno trattati come file infetti. Software che includono componenti adware potrebbero bloccarsi se questa opzione è attiva.
Scansione spyware	Esegue la scansione per minacce spyware conosciuti. Questi file verranno trattati come file infetti.
Scansione applicazione	Cerca applicazioni legittime che possono essere usate come strumenti per spiare, per nascondere applicazioni maligne o per altri intenti maligni.

Opzione	Descrizione
Scansione dialers	Esegue la scansione per applicazioni che utilizzano numeri di telefono a costo elevato. Questi file verranno trattati come file infetti. Software che includono componenti dialer potrebbero bloccarsi se questa opzione fosse attiva.
Scansione per i Rootkits	Esegue la scansione per oggetti nascosti (file e processi), generalmente conosciuti come rootkits.

- **Opzioni di scansione virus.** Specificare il tipo di oggetti da esaminare (tipi di file, archivi e così via) selezionando opzioni appropriate dalla categoria **Opzioni di scansione virus**.

Opzione		Descrizione
Esamina file	**Tutti i file**	Verranno esaminati tutti i file, indipendentemente dalla loro tipologia.
	Esaminare solo i program file	Per esaminare soltanto i file di programma. Ciò significa solo i file con le seguenti estensioni: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`; `chm`; `lnk`; `pif`; `prc`; `url`; `smm`; `pdf`; `msi`; `ini`; `csc`; `cmd`; `bas`; `eml` e `nws`.
	Estensioni definite dall'utente	Verranno esaminati soltanto i file con le estensioni specificate dall'utente. Le varie estensioni devono essere separate da ";".
Esamina i programmi impaccati		Per esaminare i file impaccati.
Esamina gli archivi		Scansiona negli archivi regolari, tipo `.zip`, `.rar`, `.ace`, `.iso` e altri. Selezionare la casella di controllo **Scansiona programmi di installazione e archivi chm** se si desidera scansionare questo tipo di file. La scansione dei file archiviati incrementa il tempo di scansione e richiede più risorse di sistema. È possibile impostare una dimensione massima di archivi da scansionare in kilobyte (KB) digitando la

Opzione	Descrizione
	dimensione in questo campo **Limite di dimensione degli archivi da scansionare**.
Scansionare gli archivi di e-mail	Per eseguire la scansione all'interno degli archivi di posta.
Esamina settore di boot	Per esaminare i settori di avvio del sistema.
Scansione della memoria	Scansiona la memoria alla ricerca di virus e altro malware.
Scansione registro	Scansione di voci di registro.
Scansionare cookies	Scansione di file cookie.

- **Opzioni di azione.** Specificare le azioni da intraprendere per ogni categoria dei file rilevati usando le opzioni in questa categoria.

Nota

Per impostare una nuova azione, fare clic sulla **Prima azione** attuale e selezionare l'opzione desiderata dal menu. Specificare una **Seconda azione** che sarà intrapresa qualora la prima non riuscisse.

▶ Selezionare l'azione da intraprendere sui file infetti rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file infetti. Questi file appariranno nel file di rapporto.
Disinfetta i file	Rimuovere il codice malware dai file infetti rilevati.
Cancella i file	Cancella immediatamente i file infetti, senza alcun avviso.
Muova i files in Quarantena	Sposta i file infetti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.

▶ Selezionare l'azione da intraprendere sui file sospetti rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file sospetti. Questi file appariranno nel file di report.

Azione	Descrizione
Cancella i file	Cancella immediatamente i file sospetti, senza alcun avviso.
Muova i files in Quarantena	Sposta i file sospetti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.

Nota
La Scansione euristica ha rilevato dei file sospetti. Vi consigliamo di inviarli al laboratorio di BitDefender.

- Selezionare l'azione da intraprendere sugli oggetti nascosti (rootkits) rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file nascosti. Questi file appariranno nel file di report.
Rinomina i files	Cambia il nome di file nascosti aggiungendo `.bd.ren` al loro nome. Come risultato, si potrà cercare tali file sul computer, se ve ne sono.
Muova i files in Quarantena	Sposta i file nascosti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.

Nota
Notare che i file nascosti non sono i file che l'utente ha nascosto in modo deliberato da Windows. Sono file nascosti da programmi speciali, noti come rootkit. I rootkit non sono file di tipo nocivo. Tuttavia sono utilizzati per rendere introvabili virus o spyware per normali programmi antivirus.

- **Opzioni per file protetti da password e criptati.** File criptati utilizzando Windows potrebbero essere importanti. Ecco perché è possibile configurare differenti azioni da intraprendere per file infetti o sospetti che sono criptati utilizzarti Windows. Un'altra categoria di file che richiede azioni speciali sono gli archivi protetti da password. Gli archivi protetti da password non possono essere esaminati a meno che non forniate la password. Utilizzare queste opzioni per configurare le azioni da intraprendere per archivi protetti da password e per file criptati con Windows.
  - **Azione da intraprendere quando viene rilevato un file criptato infetto.** Selezionare l'azione da intraprendere su file infetti criptati usando Windows. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Registra solamente i file infetti che sono criptati utilizzando Windows. Dopo che la scansione sia stata completata, potrete aprire il log di scansione per visualizzare le informazioni su questi file.
Disinfetta i file	Rimuovere il codice malware dai file infetti rilevati. La disinfezione può fallire in alcuni casi, come quando il file infetto è all'interno di specifici archivi di posta.
Cancella i file	Rimuovere immediatamente dal disco i file infetti, senza alcun avviso.
Muova i files in Quarantena	Spostare i file infetti dalla loro posizione originale alla cartella di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.

- **Azione da intraprendere quando viene rilevato un file criptato sospetto.** Selezionare l'azione da intraprendere su file sospetti criptati usando Windows. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Registra solamente i file sospetti che sono criptati utilizzando Windows. Dopo che la scansione sia stata completata, potrete aprire il log di scansione per visualizzare le informazioni su questi file.
Cancella i file	Cancella immediatamente i file sospetti, senza alcun avviso.
Muova i files in Quarantena	Sposta i file sospetti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.

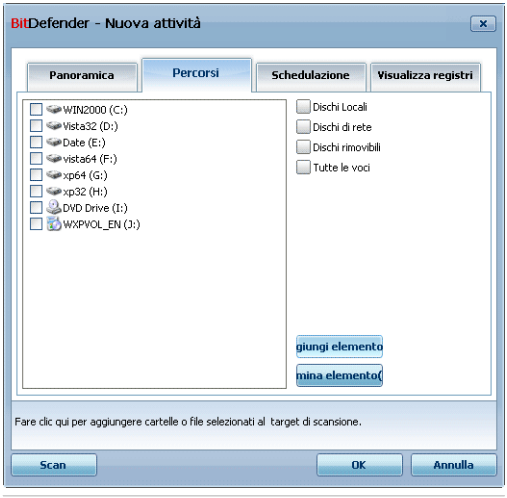
- **Azione da intraprendere quando viene rilevato un file protetto da password.** Selezionare l'azione da intraprendere sui file protetti da password rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Registra solo	Tenere registro solo dei file protetti da password nel log di scansione Dopo che la scansione sia stata completata, potrete aprire il log di scansione per visualizzare le informazioni su questi file.
Chiedere password	Quando viene rilevato un file protetto da password, chiedere all'utente di fornire la password per poter esaminare il file.

Se clicchi su **Predefinito** verranno applicate le impostazioni di default. Selezionare **OK** per salvare le modifiche e chiudere la finestra.

Impostazione del Target di Scansione

Per impostare il target di scansione a una attività di scansione specifica di un utente, fare clic con il pulsante di destra e selezionare **Percorsi**. Alternativamente, se si è già nella finestra Proprietà di un'attività, selezionare la scheda **Percorsi**. Apparirà la finestra seguente:



Target di scansione

Potete vedere la lista di dischi locali, di rete e rimuovibili, ed anche i file e cartelle aggiunti in precedenza, se ci sono. Tutti gli oggetti selezionati verranno esaminati all'esecuzione della funzione.

Sono disponibili i seguenti tasti:

- **Aggiungi Oggetti** - apre una finestra di visualizzazione dove è possibile selezionare i file o le cartelle che si desidera esaminare.

Nota
Utilizzare seleziona & trascina per aggiungere file/cartelle all'elenco.

- **Cancellare Oggetti** - rimuove il (i) file / cartella(e) precedentemente selezionati dall'elenco degli oggetti da esaminare.

Nota
Possono essere cancellati solo i file / cartelle aggiunti successivamente e non quelli "visti" automaticamente da BitDefender.

Oltre a questi pulsanti, vi sono altre opzioni che permettono la selezione veloce delle posizioni di scansione.

- **Dischi locali** - per esaminare i drives locali.
- **Dischi di rete** - per esaminare tutti i drive di rete.
- **Drive Rimovibili** - per esaminare i drive rimovibili (CD-ROM, floppy-disk).
- **Tutti gli elementi** - per esaminare tutti i drive, indipendentemente dal fatto che siano locali, sulla rete o rimovibili.

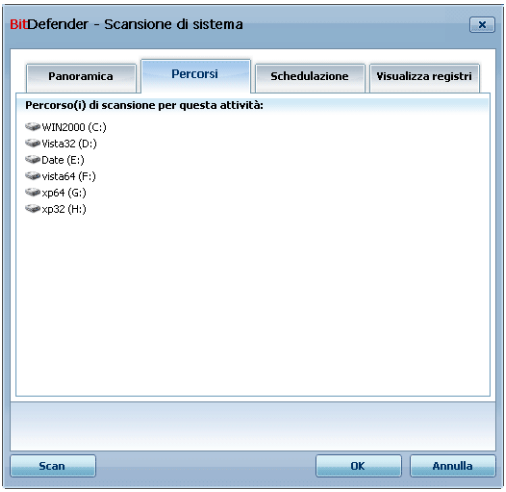
Nota
Se desiderate eseguire una scansione di tutto il vostro computer alla ricerca di virus, selezionare la casella corrispondente a **Tutti gli elementi**.

Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scansione**.

Visualizzazione del Target di Scansione delle Funzioni del Sistema

Non è possibile modificare il target di scansione delle attività di scansione dalla categoria **Attività di Sistema**. Potete solo visualizzare il loro target di scansione.

Per visualizzare il target di scansione di una specifica attività di scansione del sistema, fare clic con il tasto destro sull'attività e selezionare **Mostra Percorsi di Scansione**. Per **Scansione del sistema**, ad esempio, apparirà la seguente finestra:



Target di Scansione della Scansione del Sistema

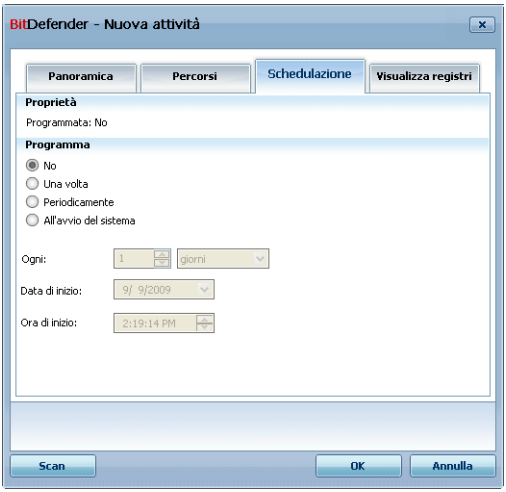
Scansione del sistema e **Scansione approfondita del sistema** scansioneranno tutti i drive locali, mentre **Scansione veloce del sistema** scansionerà solo le cartelle `Windows` e `Program Files`.

Selezionare **OK** per chiudere la finestra. Per eseguire la funzione, cliccare semplicemente **eseguire scansione**.

Programmazione delle Funzioni di Scansione

Una scansione completa può richiedere un certo tempo e agisce meglio se vengono chiusi tutti gli altri programmi. La miglior cosa da fare è programmare la scansione nel momento in cui il vostro computer non viene utilizzato.

Per vedere il programma di un'attività specifica o per modificarlo, fare clic con il pulsante destro sull'attività e selezionare **Programmazione**. Se si è già nella finestra Proprietà dell'attività, selezionare la scheda **Utilità di pianificazione**. Apparirà la finestra seguente:



Schedulazione

Potete vedere la programmazione delle funzioni, se ci sono.

Quando programmate un compito, dovete scegliere una delle seguenti opzioni:

- **No** - lancia la scansione solo quando richiesta dall'utente.
- **Una volta** - lancia la scansione solo una volta, in un certo momento. Specificare la data e l'ora di avvio nel campo **Start Date/Time**.
- **Periodicamente** - lancia la scansione periodicamente, a certi intervalli di tempo (minuti, ore, giorni, settimane, mesi) iniziando da una certa data ed ora specificate.

  Se si desidera che la scansione venga ripetuta a determinati intervalli, selezionare la casella corrispondente a **Periodicamente** e digitare nel campo **Ogni** il numero di minuti / ore / giorni / settimane / mesi indicando la frequenza del processo. È inoltre necessario specificare la data e l'ora di inizio nei campi **Data/Ora di inizio**.
- **All'avvio del sistema** - lancia la scansione un numero specifico di minuti dopo che l'utente ha effettuato l'accesso a Windows.

Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scansione**.

18.2.5. Scansione file e cartelle

Prima di iniziare il processo di scansione, assicurarsi che BitDefender sia aggiornato con le firme malware. Eseguire la scansione usando un database delle impronte obsoleto può impedire BitDefender di rilevare nuovo malware, trovato dopo l'ultimo

aggiornamento. Per verificare quando è stato eseguito l'ultimo aggiornamento, fare clic su **Aggiornamento>Aggiornamento** in Visualizzazione avanzata.

Nota

Per consentire a BitDefender di eseguire una scansione completa, dovrete chiudere tutti i programmi aperti. E' soprattutto importante chiudere il vostro client di posta (come Outlook, Outlook Express oppure Eudora).

Consiglio di scansione

Ecco altri consigli sulla scansione che potrebbero essere utili:

- In base alla dimensione del disco rigido, l'esecuzione di una scansione comprensiva del computer (ad esempio una Scansione approfondita del sistema o una Scansione del sistema) potrebbe richiedere molto tempo (fino ad un ora o più). Quindi, si dovrebbero eseguire tali scansioni quando non si usa il computer per un lungo periodo di tempo (ad esempio di notte).

  È possibile programmare la scansione affinché inizi quando è più conveniente. Assicurarsi di lasciare il computer accesso. Con Windows Vista, assicurarsi che il computer non sia nella modalità sospensione quando l'attività deve essere eseguita.

- Se si scaricano spesso file da Internet ad una cartekka specifica, si consiglia di creare una nuova attività di scansione e impostare quella cartella come target della scansione. Programmare l'attività affinché venga eseguita una volta al giorno o più spesso.

- Esiste un malware che si imposta per essere eseguito ad ogni avvio del sistema modificando le impostazioni di Windows. Per proteggere il computer da un tale malware, è possibile programmare che l'attività **Scansioen accesso automatico** venga eseguito all'avvio del sistema. Notare che la scansione accesso automatico potrebbe influenzare la performance del sistema per un breve periodo di tempo dopo l'avvio.

Metodi di Scansione

BitDefender consente quattro tipi di scansione a richiesta:

- Scansione immediata - avvia immediatamente un processo di scansione dal sistema / funzioni utente.
- Scansione contestuale - fare clic con il pulsante destro su un file o una cartella e selezionare **Scansione con BitDefender**.
- Scansione Seleziona & Trascina - seleziona & trascina un file o una cartella sopra la Barra delle Attività di Scansione.
- Scansione manuale - Utilizzare Scansione Manuale di BitDefender per selezionare direttamente i file o cartella da esaminare.

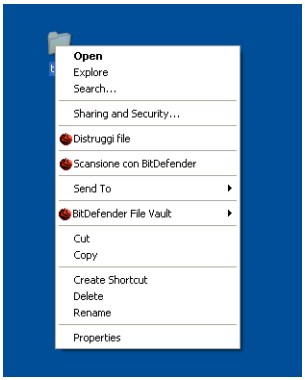
Scansione Immediata

Per eseguire una scansione del vostro computer o di parte di essi potete usare i compiti di scansione di default oppure i vostri propri compiti di scansione. Ciò si chiama scansione immediata

Per eseguire una scansione di sistema o definita dall'utente, fare clic sul pulsante **Esegui Attività** corrispondente. La Procedura guidata scansione antivirus apparirà e guiderà attraverso il processo di scansione.

Scansione Contestuale

Per esaminare un file o cartella senza configurare un nuovo compito di scansione, si può usare il menu contestuale. ciò si chiama scansione contestuale



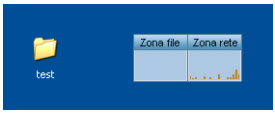
Scansione contestuale

Fare clic con il pulsante destro del mouse sul file o la cartella che si desidera scansionare e selezionare **Scansiona con BitDefender**. La Procedura guidata scansione antivirus apparirà e guiderà attraverso il processo di scansione.

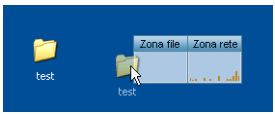
E' possibile modificare e vedere il file di report dalla finestra delle **Proprietà** del **Menu Scansione Contestuale**.

Scansione Seleziona e Trascina

Selezionare il file o la cartella che si desidera esaminare e trascinarla sulla **Barra delle Attività di Scansione**, come nella figura seguente.



Trascinare il file



Abbandonare il file

La Procedura guidata scansione antivirus apparirà e guiderà attraverso il processo di scansione.

Scansione Manuale

La scansione manuale consiste in selezionare direttamente l'oggetto da esaminare, utilizzando l'opzione Scansione Manuale BitDefender dal gruppo di programmi BitDefender nel Menu di Avvio.

Nota
La scansione manuale è molto utile, poichè può essere eseguita anche quando Windows lavora in Modalità Provvisoria.

Per selezionare l'oggetto da scansionare con BitDefender, nel menu Avvio di Windows, seguire il percorso **Avvio → Programmi → BitDefender 2010 → Scansione Manuale di BitDefender**. Apparirà la finestra seguente:

BitDefender Total Security 2010
Scansione Antivirus
Elementi scansionati:
Fare clic su Aggiungi Target per definire il target di scansione per questa attività di scansione.
Aggiunge cartelle
Target di scansione:
In questo passaggio, è possibile scegliere i file e le cartelle da scansionare.
bitdefender
Annulla
Continua

Scansione Manuale

Fare clic su **Aggiungi Cartella**, selezionare la posizione per cui si desidera eseguire la scansione e fare clic su **OK**. Se si desidera eseguire la scansione di cartelle multiple, ripetere questa azione per ciascuna posizione aggiuntiva.

I percorsi alle posizioni selezionate appariranno nella colonna **Target di Scansione**. Se si cambia idea circa la locazione, sarà sufficiente fare clic sul pulsante **Rimuovere** vicino. Fare clic sul pulsante **Rimuovi Tutti i Percorsi** per rimuovere tutte le posizioni aggiunte all'elenco.

Quando si ha concluso la selezione delle posizioni, fare clic su **Continua**. La Procedura guidata scansione antivirus apparirà e guiderà attraverso il processo di scansione.

Procedura guidata scansione antivirus

Quando si avvia la scansione su richiesta, apparirà la Procedura guidata Scansione Antivirus. Seguire la procedura di tre passi per completare il processo di scansione.

Nota

Se non appare la procedura guidata di scansione, potrebbe darsi che la procedura guidata sia configurata per una esecuzione sullo sfondo. Cercare l'icona di avanzamento della scansione nella barra delle applicazioni. Clicca su questa icona per aprire un processo di scansione e visualizzarne il progresso.

Passo 1/3 – Scansione

BitDefender inizierà la scansione degli oggetti selezionati.

Scansione in corso

Potete visualizzare lo stato della scansione e le statistiche (velocità di scansione, tempo trascorso, numero di oggetti esaminati / infetti / sospetti / nascosti ed altro).

Attendere che BitDefender finisca la scansione.

Nota
La durata del processo dipende dalla complessità della scansione.

Archivi protetti da password. Se BitDefender rileva un archivio protetto da password durante la scansione e l'azione predefinita è **Richiedi la password**, verrà chiesto di inserire la password. Gli archivi protetti da password non possono essere esaminati a meno che non forniate la password. Sono disponibili le seguenti opzioni:

- **Password.** Se si desidera che BitDefender scansioni l'archivio, selezionare questa opzione e digitare la password. Se non si conosce la password, scegliere un'altra opzione.
- **Non chiedere una password e ignorare questo oggetto durante la scansione.** Selezionare questa opzione per non scansionare questo archivio.
- **Ignora tutti gli elementi protetti da password senza scansionarli.** Selezionare questa opzione se non si vuole ricevere ulteriore domande sugli

archivi protetti da password. BitDefender non sarà in grado di scansionarli, ma verranno annotati nel registro della scansione.

Fare clic su **OK** per continuare la scansione.

Arresto o messa in pausa della scansione. Potete fermare la scansione in qualsiasi momento, cliccando su **Fermare**. Verrete portati all'ultimo passo dell'assistente. Per interrompere temporaneamente il processo di scansione, cliccare semplicemente su **Pausa**. Per riprendere la scansione dovrete cliccare su **Continuare**.

Passo 2/3 – Selezionare Azioni

Una volta completato il processo di scansione, apparirà una nuova finestra, dove potrete visualizzare i risultati della scansione.

BitDefender Total Security 2010 - Scansione approfondita del sistema
Scansione Antivirus
Sommario dei Risultati
Sotto è possibile trovare sommari di risultati per l'attività attuale di scansione.
Problemi risolti: 0
1 minacce che interessano 1 oggetto(i) richiedono attenzione.
Intraprendi un'azione generale per tutti gli elementi non risolti o seleziona individualmente l'azione per ogni elemento:
Scegli una azione:
EICAR-Test-File (not a virus)
1 problema rimanente (disinfezione fallita)
Scegli una azione:
BitDefender ha rilevato e bloccato dei virus sul computer! Questo è l'elenco delle minacce. Fare clic sul nome del virus per vedere il relativo elenco di elementi infetti.
bitdefender
Continua

Azioni

Si potrà vedere il numero di problemi che colpiscono il vs. sistema.

Gli oggetti infetti vengono mostrati in gruppi in base al malware con il quale sono stati infettati. Cliccare sul link corrispondente alla minaccia per trovare più informazioni sugli oggetti infetti.

Potete scegliere di intraprendere un'azione globale per tutti i problemi oppure selezionare azioni separate per ogni gruppo di problemi.

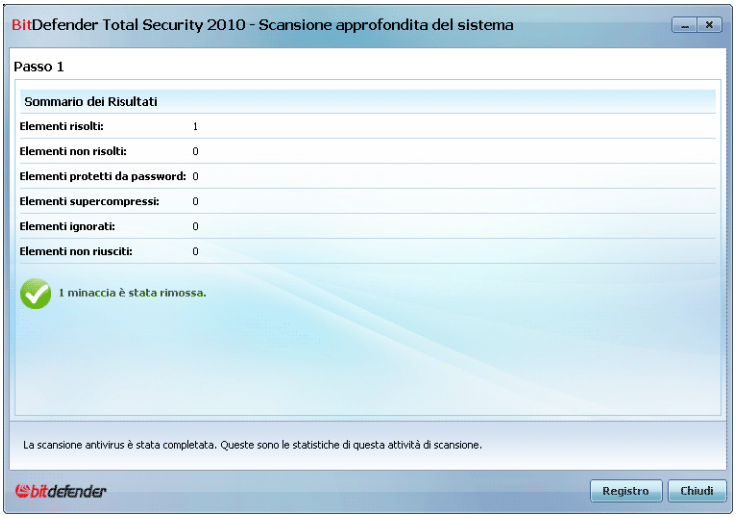
Una o più delle seguenti opzioni possono apparire nel menu:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file rilevati. Dopo che la scansione sia stata completata, potrete aprire il log di scansione per visualizzare le informazioni su questi file.
Disinfettare	Rimuove il codice malware da file infetti.
Eliminare	Elimina i file infetti.
Sposta in quarantena	Sposta i file infetti nella quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.
Rinomina i files	Cambia il nome di file nascosti aggiungendo `.bd.ren` al loro nome. Come risultato, si potrà cercare tali file sul computer, se ve ne sono. Notare che i file nascosti non sono i file che l'utente ha nascosto in modo deliberato da Windows. Sono file nascosti da programmi speciali, noti come rootkit. I rootkit non sono file di tipo nocivo. Tuttavia sono utilizzati per rendere introvabili virus o spyware per normali programmi antivirus.

Cliccare su **Continuare** per applicare le azioni specificate.

Passo 3/3 – Visualizzare risultati

Quando BitDefender completa la risoluzione dei problemi, i risultati della scansione appariranno in una nuova finestra.


BitDefender Total Security 2010 - Scansione approfondita del sistema
Passo 1
Sommario dei Risultati
Elementi risolti: 1
Elementi non risolti: 0
Elementi protetti da password: 0
Elementi supercompressi: 0
Elementi ignorati: 0
Elementi non riusciti: 0
1 minaccia è stata rimossa.
La scansione antivirus è stata completata. Queste sono le statistiche di questa attività di scansione.
bitdefender
Registro
Chiudi

Riassunto

E' possibile visualizzare il sommario dei risultati. Se si desiderano informazioni esaurienti sul processo di scansione, fare clic su **Visualizza registro** per visualizzare il registro di scansione.

Importante
Se richiesto, vi preghiamo di riavviare il sistema per completare il processo di pulizia.

Cliccare su **Chiudere** per chiudere la finestra.

BitDefender potrebbe non risolvere alcuni problemi

Nella maggior parte dei casi BitDefender disinfetta con successo i file infetti che rileva o isola l'infezione. Comunque, ci sono dei problemi che non possono essere risolti.

In questi casi vi consigliamo di contattare il Team di supporto di BitDefender su www.bitdefender.it. Il nostro team di supporto vi aiuterà a risolvere i vostri problemi.

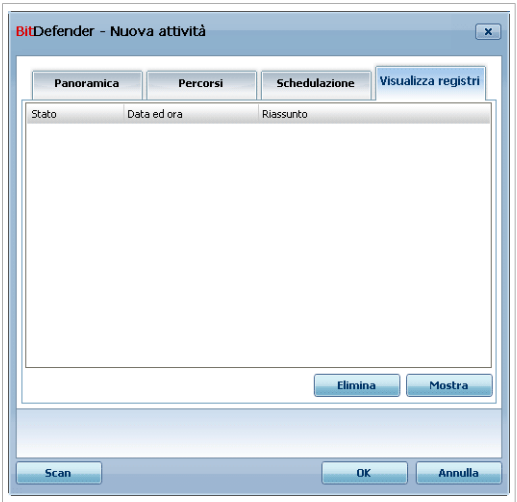
BitDefender ha rilevato dei file sospetti.

I file sospetti sono file rilevati dall'analisi euristica come potenzialmente infetti con malware la cui firma non è ancora stata rilasciata.

Se sono stati rilevati file sospetti durante la scansione, vi sarà richiesto di inviarli al Lab BitDefender. Cliccare su **OK** per inviare questi file ai laboratori BitDefender per ulteriori analisi.

18.2.6. Visualizzazione dei Registri di Scansione

Per visualizzare i risultati della scansione una volta completata un'attività, fare clic con il tasto destro sull'attività e selezionare **Visualizza Registri**. Apparirà la finestra seguente:



Esaminare registri

Qui potete trovare i file del report generati ogni che una funzione viene eseguita. In ogni file vengono fornite informazioni sullo stato del processo di scansione registrato, la data e l'ora in cui la scansione è stata eseguita ed un riassunto sui risultati della scansione.

Sono disponibili due pulsanti:

- **Cancellare** - per eliminare il log di scansione selezionato.
- **Mostrare** - per visualizzare il log di scansione selezionato. Il registro di scansione si aprirà nel vostro web browser predefinito.

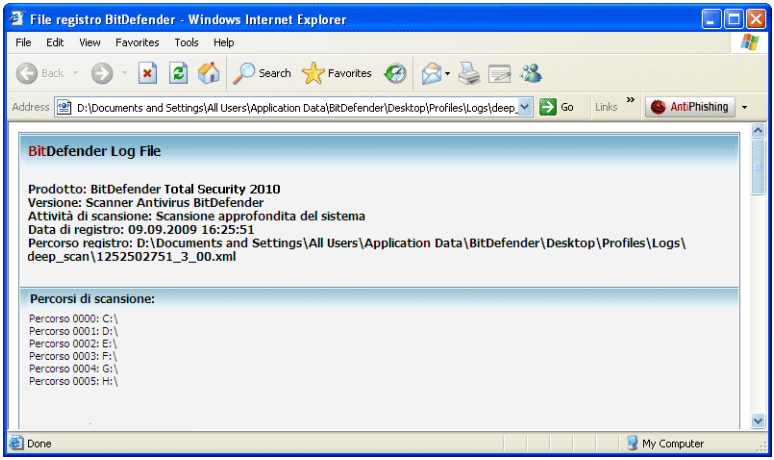
Nota

Inoltre, per visualizzare o cancellare un file, fare clic con il pulsante destro sul file e selezionare l'opzione corrispondente dal menu di scelta rapida.

Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scansione**.

Esempio di Registro di Scansione

La seguente figura rappresenta un esempio di registro di scansione:



Esempio di Registro di Scansione

Il log di scansione contiene informazioni dettagliate sul processo di scansione registrato, sul target di scansione, le minacce individuate e le azioni intraprese su queste minacce.

18.3. Oggetti esclusi dalla scansione

Ci sono dei casi in cui si può avere bisogno di escludere certi file dalla scansione. Ad esempio, si può volere escludere un file di testo EISCAR dalla scansione all'accesso, oppure i file `.avi` dalla scansione a richiesta.

BitDefender permette di escludere oggetti dalle scansioni all'accesso ed a richiesta, o da entrambi. Questa caratteristica cerca di ridurre i tempi di scansione e di evitare le interferenze con il vostro lavoro.

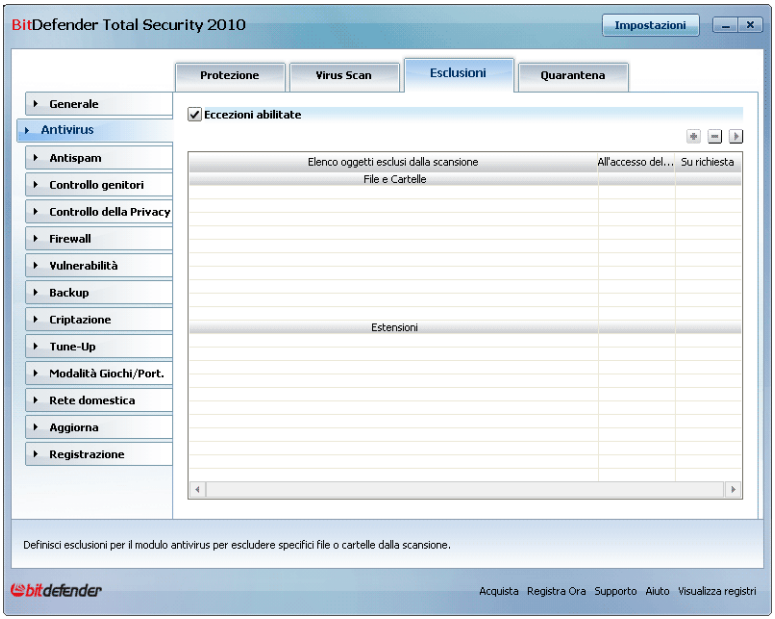
Due tipi di oggetti possono essere esclusi dalla scansione:

- **Percorsi** - Il file o cartella (inclusi tutti gli oggetti che essi contiene) indicato da un percorso specifico verrà escluso dalla scansione.
- **Estensioni** - tutti i file che hanno una specifica estensione verranno esclusi dalla scansione.

Nota

Gli oggetti esclusi dalla scansione all'accesso non verranno esaminati, non importa se sono visitati da voi o da un'applicazione.

Per visualizzare e gestire gli oggetti esclusi dalla scansione, fare clic su **Antivirus>Eccezioni** in Modalità Avanzata.



Eccezioni

Si possono visualizzare gli oggetti (file, cartelle, estensioni) esclusi dalla scansione. Potete vedere se ogni oggetto è stato escluso dalla scansione all'accesso, dalla scansione a richiesta o da entrambi.

Nota

Le eccezioni qui specificate NON verranno applicate nella scansione contestuale. La scansione contestuale è un tipo di scansione su richiesta: fare clic con il pulsante destro sul file o cartella che si vuole scansionare e selezionare **Scansiona con BitDefender**.

Per rimuovere una voce dalla tabella, selezionarla e fare clic sul pulsante **Elimina**.

Per modificare una voce dalla tabella, selezionarla e fare clic sul pulsante **Modifica**. Apparirà una nuova finestra dove si potrà modificare l'estensione od il percorso da

escludere ed il tipo di scansione dal quale escluderlo, a seconda delle necessità. Apportare le necessarie modifiche e cliccare **OK**.

Nota

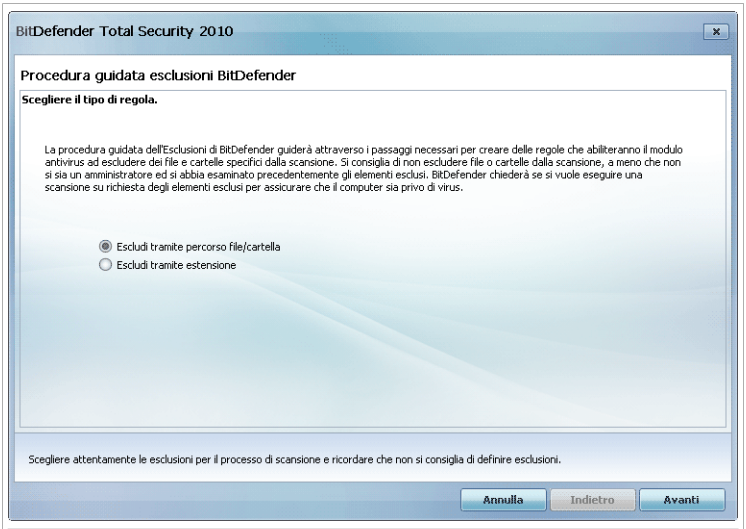
È inoltre possibile fare clic con il pulsante destro sull'oggetto ed utilizzare le opzioni del menu di scelta rapida per modificarlo o eliminarlo.

Potete cliccare su **Ignorare** per ritornare alla situazione precedente alle modifiche effettuate alla tabella delle regole, sempre che non le abbiate salvate cliccando su **Applicare**.

18.3.1. Esclusione dei Percorsi dalla Scansione

Per escludere dei percorsi dalla scansione, fare clic sul pulsante **Aggiungi**. Verrete guidati dall'assistente di configurazione attraverso il processo di esclusione dei percorsi dalla scansione.

Passo 1/4 – Selezionare tipo di oggetto


BitDefender Total Security 2010
Procedura guidata esclusioni BitDefender
Scegliere il tipo di regola.
La procedura guidata dell'Esclusioni di BitDefender guiderà attraverso i passaggi necessari per creare delle regole che abiliteranno il modulo antivirus ad escludere dei file e cartelle specifici dalla scansione. Si consiglia di non escludere file o cartelle dalla scansione, a meno che non si sia un amministratore ed si abbia esaminato precedentemente gli elementi esclusi. BitDefender chiederà se si vuole eseguire una scansione su richiesta degli elementi esclusi per assicurare che il computer sia privo di virus.
Escludi tramite percorso file/cartella
Escludi tramite estensione
Scegliere attentamente le esclusioni per il processo di scansione e ricordare che non si consiglia di definire esclusioni.
Annulla
Indietro
Avanti

Tipo di Oggetto.

Selezionare l'opzione di escludere un percorso dalla scansione.

Selezionare **Avanti**.

Passo 2/4 – Specificare i percorsi esclusi

BitDefender Total Security 2010
Procedura guidata esclusioni BitDefender
Escludi percorsi
Inserire qui il percorso che si deve escludere e fare clic su Aggiungi.
Sfoglia
Aggiungi
Percorsi selezionati
c:\
Sopra è possibile cercare il percorso da escludere dalla scansione. Assicurarsi di fare clic su Aggiungi dopo aver scelto un percorso escluso (file o cartelle). È possibile aggiungere più elementi a questo elenco.
Scegliere attentamente le esclusioni per il processo di scansione e ricordare che non si consiglia di definire esclusioni.
Annulla
Indietro
Avanti

Percorsi Esclusi

Per specificare i percorsi da escludere dalla scansione, utilizzare uno dei seguenti metodi:

- Cliccare **Sfoglia**, selezionare il file o cartella che volete venga escluso dalla scansione e quindi cliccare su **Aggiungere**.
- Scrivere il percorso che volete venga escluso dalla scansione nel campo modifica e cliccare **Aggiungere**.

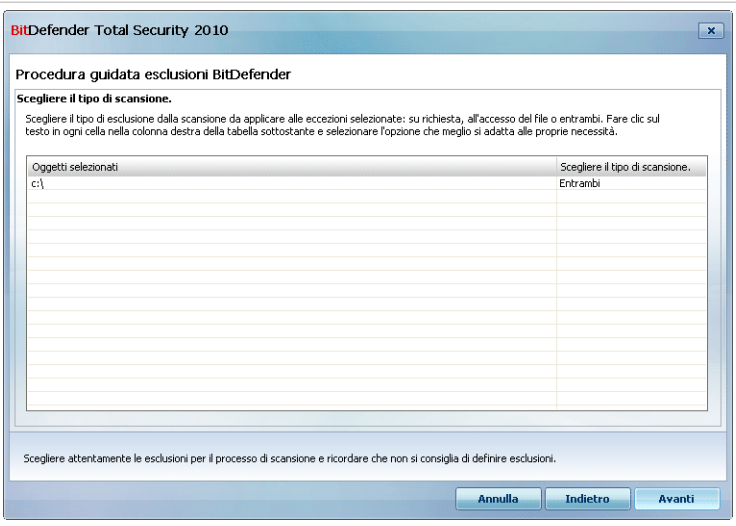
> **Nota**
> Se il percorso inserito non esiste, comparirà un messaggio di errore. Cliccare **OK** e controllare la validità del percorso.

I percorsi appariranno nella tabella man mano che vengono aggiunti. Potete aggiungere quanti percorsi volete.

Per rimuovere una voce dalla tabella, selezionarla e fare clic sul pulsante **Elimina**.

Selezionare **Avanti**.

Passo 3/4 – Selezionare tipo di scansione


BitDefender Total Security 2010
Procedura guidata esclusioni BitDefender
Scegliere il tipo di scansione.
Scegliere il tipo di esclusione dalla scansione da applicare alle eccezioni selezionate: su richiesta, all'accesso del file o entrambi. Fare clic sul testo in ogni cella nella colonna destra della tabella sottostante e selezionare l'opzione che meglio si adatta alle proprie necessità.
Oggetti selezionati
Scegliere il tipo di scansione.
c:\
Entrambi
Scegliere attentamente le esclusioni per il processo di scansione e ricordare che non si consiglia di definire esclusioni.
Annulla
Indietro
Avanti

Tipo di Scansione

Potete vedere una tabella contenente i percorsi da escludere dalla scansione ed il tipo di scansione dal quale vengono esclusi.

Per default i percorsi selezionati verranno esclusi da entrambe le scansioni, all'accesso ed a richiesta. Per modificare quando applicare l'eccezione, cliccare nella colonna di destra e selezionare dall'elenco l'opzione desiderata.

Selezionare **Avanti**.

Passo 4/4 – Esaminare i file esclusi

BitDefender Total Security 2010
Procedura guidata esclusioni BitDefender
Termina
Prima di escludere un file da una scansione, di consiglia vivamente di verificare che non abbia virus. Se si abilita questa opzione, alla fine della procedura guidata verrà eseguita una scansione Antivirus.
Selezionarlo se si desidera che l'attività di scansione si avvii quando si fa clic su Fine.
Scegliere attentamente le esclusioni per il processo di scansione e ricordare che non si consiglia di definire esclusioni.
Annulla
Indietro
Termina

Scansione dei File Esclusi

E' altamente consigliato esaminare i file nei percorsi specificati per essere sicuri che non siano infetti. Selezionare l'opzione di escludere un percorso dalla scansione.

Selezionare **Termina**.

18.3.2. Esclusione delle Estensioni dalla Scansione

Per escludere delle estensioni dalla scansione, fare clic sul pulsante **Aggiungi**. Verrete guidati dall'assistente di configurazione attraverso il processo di esclusione delle estensioni dalla scansione.

Passo 1/4 – Selezionare tipo di oggetto

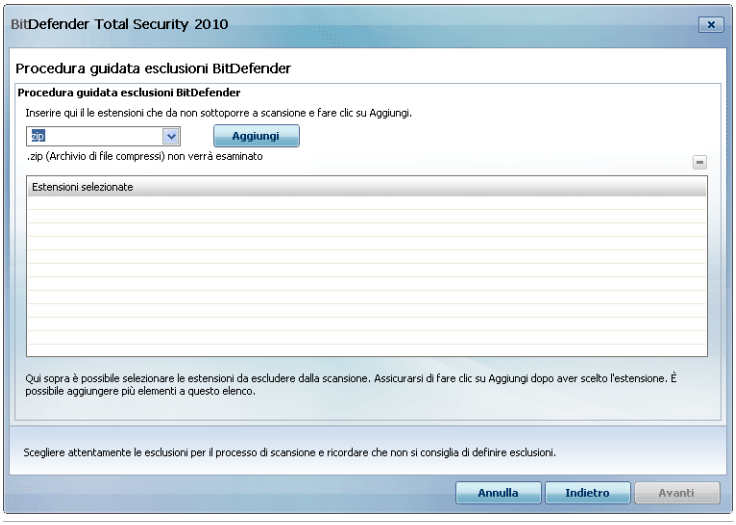
BitDefender Total Security 2010
Procedura guidata esclusioni BitDefender
Scegliere il tipo di regola.
La procedura guidata dell'Esclusioni di BitDefender guiderà attraverso i passaggi necessari per creare delle regole che abiliteranno il modulo antivirus ad escludere dei file e cartelle specifici dalla scansione. Si consiglia di non escludere file o cartelle dalla scansione, a meno che non si sia un amministratore ed si abbia esaminato precedentemente gli elementi esclusi. BitDefender chiederà se si vuole eseguire una scansione su richiesta degli elementi esclusi per assicurare che il computer sia privo di virus.
Escludi tramite percorso file/cartella
Escludi tramite estensione
Scegliere attentamente le esclusioni per il processo di scansione e ricordare che non si consiglia di definire esclusioni.
Annulla
Indietro
Avanti

Tipo di Oggetto.

Selezionare l'opzione di escludere estensioni dalla scansione.

Selezionare **Avanti**.

Passo 2/4 – Specificare le estensioni escluse


BitDefender Total Security 2010
Procedura guidata esclusioni BitDefender
Procedura guidata esclusioni BitDefender
Inserire qui il le estensioni che da non sottoporre a scansione e fare clic su Aggiungi.
Aggiungi
.zip (Archivio di file compressi) non verrà esaminato
Estensioni selezionate
Qui sopra è possibile selezionare le estensioni da escludere dalla scansione. Assicurarsi di fare clic su Aggiungi dopo aver scelto l'estensione. È possibile aggiungere più elementi a questo elenco.
Scegliere attentamente le esclusioni per il processo di scansione e ricordare che non si consiglia di definire esclusioni.
Annulla
Indietro
Avanti

Estensioni Escluse

Per specificare le estensioni da escludere dalla scansione, utilizzare uno dei seguenti metodi:

- Selezionare dal menu l'estensione che volete venga esclusa dalla scansione e quindi cliccare su **Aggiungere**.

  Nota
  Il menu contiene un elenco di tutte le estensioni registrate sul vostro sistema. Quando selezionate un'estensione, potrete vedere la sua descrizione, se disponibile.

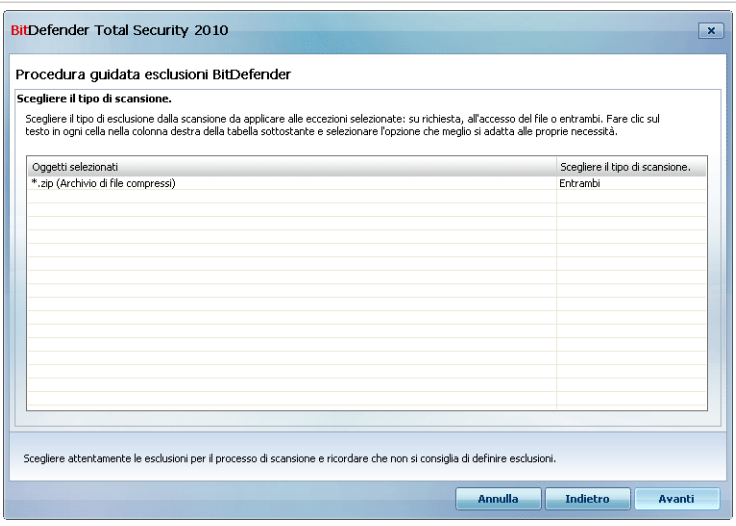
- Scrivere l'estensione che volete venga esclusa dalla scansione nel campo modifica e cliccare **Aggiungere**.

Le estensioni appariranno nella tabella man mano che vengono aggiunte. Potete aggiungere quante estensioni volete.

Per rimuovere una voce dalla tabella, selezionarla e fare clic sul pulsante **Elimina**.

Selezionare **Avanti**.

Passo 3/4 – Selezionare tipo di scansione


BitDefender Total Security 2010
Procedura guidata esclusioni BitDefender
Scegliere il tipo di scansione.
Scegliere il tipo di esclusione dalla scansione da applicare alle eccezioni selezionate: su richiesta, all'accesso del file o entrambi. Fare clic sul testo in ogni cella nella colonna destra della tabella sottostante e selezionare l'opzione che meglio si adatta alle proprie necessità.
Oggetti selezionati
Scegliere il tipo di scansione.
*.zip (Archivio di file compressi)
Entrambi
Scegliere attentamente le esclusioni per il processo di scansione e ricordare che non si consiglia di definire esclusioni.
Annulla
Indietro
Avanti

Tipo di Scansione

Potete vedere una tabella contenente le estensioni da escludere dalla scansione ed il tipo di scansione dal quale vengono escluse.

Per default le estensioni selezionate verranno escluse da entrambe le scansioni, all'accesso ed a richiesta. Per modificare quando applicare l'eccezione, cliccare nella colonna di destra e selezionare dall'elenco l'opzione desiderata.

Selezionare **Avanti**.

Passo 4/4 – Selezionare tipo di scansione

BitDefender Total Security 2010
Procedura guidata esclusioni BitDefender
Termina
Prima di escludere un file da una scansione, di consiglia vivamente di verificare che non abbia virus. Se si abilita questa opzione, alla fine della procedura guidata verrà eseguita una scansione Antivirus.
Scegliere attentamente le esclusioni per il processo di scansione e ricordare che non si consiglia di definire esclusioni.
Annulla
Indietro
Termina

Tipo di Scansione

E' altamente consigliato esaminare i file con le estensioni specificate per essere sicuri che non siano infetti.

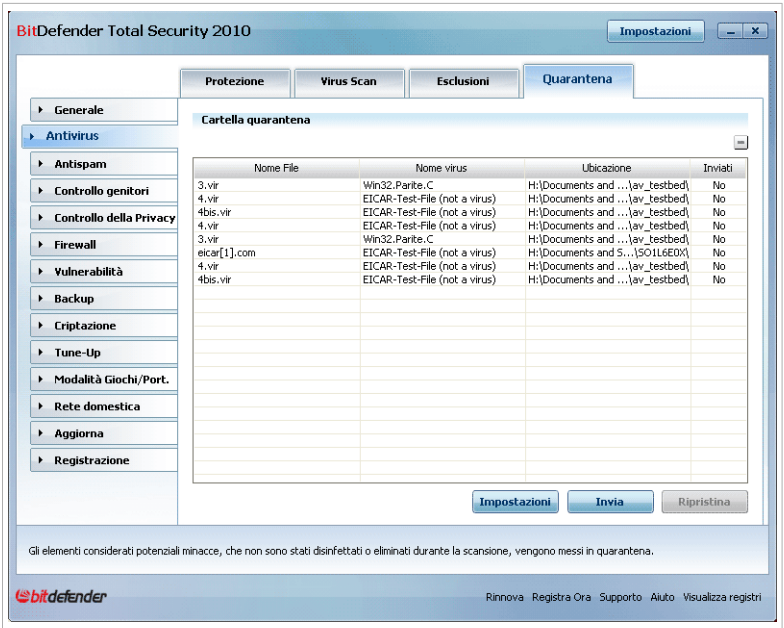
Selezionare **Termina**.

18.4. Area di Quarantena

BitDefender consente di isolare i file infetti o sospetti in un'area sicura, chiamata quarantena. Isolando questi file in quarantena, scompare il rischio di essere infettati e contemporaneamente si ha la possibilità di inviare questi file ai Laboratori BitDefender per ulteriori analisi.

Inoltre BitDefender scansiona i file in quarantena dopo ogni aggiornamento di firme malware. I file puliti vengono spostati automaticamente alla loro ubicazione originale.

Per visualizzare e gestire i file in quarantena e per configurare le impostazioni della quarantena, fare clic su **Antivirus>Quarantena** in Modalità Avanzata.



Quarantena

La sezione Quarantena mostra tutti i file attualmente isolati nella cartella Quarantena. Per ogni file in quarantena, potete vedere il suo nome, il nome del virus rilevato, il percorso alla sua posizione originale e la data di invio.

Nota
Quando un virus è in quarantena, non può più arrecare alcun danno in quanto non può essere eseguito o letto.

18.4.1. Gestione dei File in Quarantena

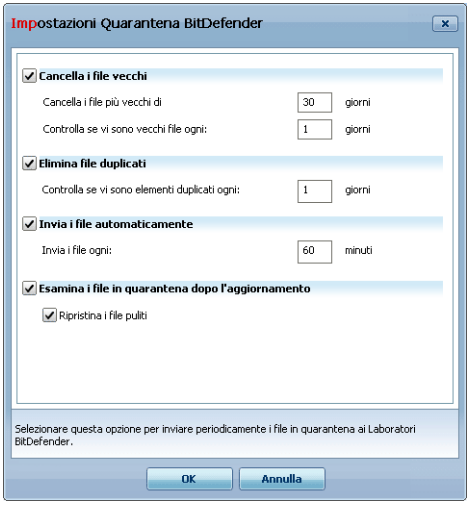
Potete inviare qualsiasi file selzionato dalla quarantena al lab BitDefender cliccando su **Invia**. Per default, BitDefender invierà automaticamente i file in quarantena ogni 60 minuti.

Per cancellare un file selezionato dalla quarantena, fare clic sul pulsante **Elimina**. Se si desidera inviare un file selezionato alla sua ubicazione originale, fare clic su **Riprisitina**.

Menù contestuale. E' disponibile un menu contestuale che vi permette di gestire facilmente i file in quarantena. Sono disponibili le stesse opzioni su menzionate. Potete anche selezionare **Aggiornare** per aggiornare la sezione di Quarantena.

18.4.2. Configurazione delle Impostazioni di Quarantena

Per configurare le impostazioni di quarantena, cliccare su **Impostazioni**. Apparirà una nuova finestra.



Impostazioni di Quarantena

Utilizzando le impostazioni di quarantena, potete configurare BitDefender per eseguire automaticamente le seguenti azioni:

Eliminare i vecchi file. Per eliminare automaticamente i vecchi file, selezionare l'opzione corrispondente. Dovete specificare il numero di giorni dopo i quali i file in quarantena devono essere eliminati e la frequenza con cui BitDefender deve effettuare il controllo dei vecchi file.

Nota
Per default, BitDefender effettuerà il controllo dei vecchi file ogni giorno ed eliminerà i file più vecchi di 30 giorni.

Elimina file duplicati. Per eliminare automaticamente i file duplicati in quarantena, selezionare l'opzione corrispondente. Dovete specificare il numero di giorni tra due controlli consecutivi dei duplicati.

Nota
Per default, BitDefender effettuerà il controllo dei file duplicati in quarantena ogni giorno.

Invio automatico dei file. Per inviare automaticamente i file in quarantena, selezionare l'opzione corrispondente. Dovete specificare la frequenza con cui inviare i file.

Nota
Per default, BitDefender invierà automaticamente i file in quarantena ogni 60 minuti.

Esaminare i file in quarantena dopo l'aggiornamento. Per esaminare automaticamente i file in quarantena dopo l'aggiornamento, selezionare l'opzione corrispondente. Potete scegliere di far tornare automaticamente i file puliti alla loro posizione originale selezionando **Ripristinare file puliti**.

Selezionare **OK** per salvare le modifiche e chiudere la finestra.

19. Antispam

Antispam BitDefender impiega notevoli innovazioni tecnologiche e filtri standard dell'industria antispam per eliminare lo spam prima che raggiunga l'Inbox dell'utente.

19.1. Approfondimenti Antispam

Lo Spam rappresenta un problema in continua crescita, sia per i privati che per le aziende. Non è piacevole, non vorreste che i vostri figli lo vedessero, potrebbe penalizzarvi (per aver sprecato troppo tempo o per aver ricevuto mail pornografiche in ufficio) e non potete impedire alla gente di inviarlo. La miglior cosa da fare, ovviamente, e di fermarne la ricezione. Sfortunatamente lo Spam si presenta sotto molte forme e dimensioni e ce n'è veramente tanto in giro.

19.1.1. Filtri Antispam

Il Motore Antispam BitDefender incorpora diversi filtri che assicurano l'assenza di SPAM nella vostra Inbox: Elenco amici, Elenco Spammers, Filtro Carattere, Filtro Immagine, Filtro URL, Filtro NeuNet (Heuristico) e Filtro Bayesiano.

Nota

E' possibile attivare/disattivare ognuno di questi filtri nel modulo **Antispam**, sezione Impostazioni.

Elenco Amici / Elenco Spammer

La maggior parte delle persone comunica regolarmente con un gruppo di persone o riceve messaggi da organizzazioni o società nello stesso dominio. Utilizzando **L'elenco Amici o Spammer**, potrete facilmente classificare da quali persone volete ricevere e-mail (Amici) indipendentemente dal contenuto del messaggio, o da quali persone non volete più ricevere nulla (spammer).

E' possibile gestire l'elenco Amici / Spammer dalla Modalità Avanzata oppure dalla Barra degli strumenti Antispam integrata in alcuni dei client di posta più comunemente usati.

Nota

Raccomandiamo di aggiungere i nomi dei vostri amici e gli indirizzi e-mail all'**elenco Amici**. BitDefender non blocca i messaggi di coloro che sono nell'elenco; aggiungere amici aiuta a garantire che i messaggi leciti vengano recapitati.

Filtro Carattere

La maggior parte dei messaggi Spam sono scritti in caratteri cirillici e/o asiatici. Il filtro Carattere rileva questo tipo di messaggi e li etichetta come SPAM.

Filtro Immagine

Da quando l'eliminazione della scansione con il Filtro Euristico è diventata una scoperta, oggigiorno le cartelle di posta in arrivo sono piene di molti messaggi contenenti solo un imagine con contenuti insoliti. Per contrastare questo crescente problema, BitDefender ha introdotto il **Filtro Immagine** che confronta le firme delle immagine delle e-mail con il database del BitDefender. In caso di riconoscimento, la e-mail verrà etichettata come Spam.

Filtro URL

La maggior parte dei messaggi Spam contiene links a vari siti web. Questi siti solitamente contengono ulteriore pubblicità e la possibilità di acquistare oggetti e, alle volte, vengono usati per phishing.

BitDefender mantiene un database di tali links. Il filtro URL esamina ogni link URL contenuto in un messaggio con il suo database. Se corrisponde, il messaggio viene etichettato come SPAM.

Filtro Euristico

Il **Filtro Euristico** esegue una serie di test a tutte le componenti del messaggio (ovvero, non solo l'intestazione ma anche il corpo del messaggio sia in formato HTML che di testo), alla ricerca di parole, frasi, links o altri elementi caratteristici dello SPAM. Basandosi sui risultati dell'analisi, esso aggiunge un punteggio SPAM al messaggio.

Il filtro rileva inoltre messaggi segnati come `ESPLICITAMENTE SESSUALE:` nell'oggetto e li etichetta come SPAM.

Nota

A partire dal 19 Maggio 2004 lo Spam contenente materiale a sfondo sessuale deve includere l'avviso `SEXUALLY-EXPLICIT` nell'oggetto, diversamente sarà passibile di sanzioni per violazione della legge federale.

Filtro Bayesiano

Il modulo **Filtro Bayesiano** classifica i messaggi secondo informazioni statistiche relative alla frequenza di specifiche parole contenute nei messaggi classificati come Spam in confronto a quelli dichiarati come non-Spam (da voi o dal filtro euristico).

Ciò significa, ad esempio, che se una determinata parola di quattro lettere appare più spesso in uno Spam, è naturale desumere che esiste una notevole possibilità che il successivo messaggio in entrata contenente la stessa parola SIA Spam. Vengono prese in considerazione tutte le parole rilevanti all'interno di un messaggio. Sintetizzando le informazioni statistiche, viene valutata la probabilità globale che l'intero messaggio sia Spam.

Questo modulo presenta un'altra interessante caratteristica: lo si può "addestrare". Si adatta velocemente alla tipologia di messaggi ricevuti da un determinato utente e immagazzina informazioni su tutto. Per funzionare efficacemente, il filtro va addestrato, ovvero gli vanno presentati esempi di Spam e di messaggi leciti, proprio come si addestra un cane a rilevare determinati odori. A volte il filtro va anche corretto – stimolato a correggersi quando prende una decisione sbagliata.

Importante

È possibile correggere il filtro bayesiano utilizzando i pulsanti **È spam** e **Non è spam** dalla Barra degli strumenti Antispam .

19.1.2. Operazione Antispam

Il motore Antispam BitDefender usa tutti i filtri antispam combinati per determinare se un certo messaggio e-mail dovrebbe giungere alla **Posta in arrivo** o no.

Importante

I messaggi spam rilevati da BitDefender sono marcati con il prefisso [SPAM] nell'oggetto. BitDefender sposta automaticamente messaggi spam ad una cartella specifica, come segue:

- In Microsoft Outlook, i messaggi spam sono spostati nella cartella **Spam**, situata nella cartella **Posta eliminata**. La cartella **Spam** è creata durante l'installazione di BitDefender.
- In Outlook Express e Windows Mail, i messaggi spam sono spostati direttamente nella cartella **Posta eliminata**.
- In Mozilla Thunderbird, i messaggi spam sono spostati nella cartella **Spam**, situata nella cartella **Cestino**. La cartella **Spam** è creata durante l'installazione di BitDefender.

Se si utilizza un altro client per la posta, è necessario creare una regola per spostare i messaggi e-mail segnati come [SPAM] da BitDefender in una cartella personalizzata di quarantena.

Ogni e-mail che arriva da Internet viene prima controllata con il filtro Elenco Amici/Elenco Spammer. Se l'indirizzo del mittente viene trovato nell'Elenco Spammer l'e-mail viene spostata direttamente nella vostra **Inbox**.

Diversamente, il filtro Elenco Spammer prenderà in carico l'e-mail per verificare se l'indirizzo del mittente è contenuto nel suo elenco. L'e-mail verrà contrassegnata come SPAM e spostata nella cartella **Spam** (situata in Microsoft Outlook) qualora il confronto con la lista abbia dato esito positivo.

Ancora, il filtro Carattere controllerà se l'e-mail è scritta con caratteri cirillici o asiatici. In questo caso l'e-mail verrà marcata come SPAM e spostata nella cartella **Spam**.

Qualora l'e-mail non fosse scritta con caratteri asiatici o cirillici, la stessa verrà passata al filtro Filtro Immagine. Il **Filtro Immagine** controllerà tutti I messaggi e-mail contenenti allegati con immagini con contenuti di spam.

Il filtro URL cercherà i link e li comparerà con i link del database di BitDefender. In caso di corrispondenza, il filtro aggiungerà un punteggio Spam alla e-mail.

Il Filtro Euristico prenderà in carico l'e-mail ed eseguirà una serie di test su tutte le componenti del messaggio, alla ricerca di parole, frasi, collegamenti o caratteristiche dello Spam. Il risultato sarà quello di aggiungere un altro punteggio Spam alla e-mail.

Nota

Se l'e-mail è marcata come SEXUALLY EXPLICIT nella riga del soggetto, BitDefender la considererà come SPAM.

Il modulo del filtro Bayesiano analizzerà ulteriormente il messaggio, basandosi su informazioni statistiche relative all'incidenza con cui determinate parole appaiono nei messaggi classificati come Spam in paragone a quelli dichiarati come non-Spam (da voi o dal filtro euristico). Verrà aggiunto un punteggio Spam alla e-mail.

Se il risultato del punteggio (punteggio URL + punteggio Euristico + punteggio Bayesiano) eccede il punteggio Spam per un messaggio (impostato dall'utente nella sezione Antispam come livello di tolleranza), il messaggio viene considerato come SPAM.

19.1.3. Aggiornamenti Antispam

Ogni volta che esegui un aggiornamento:

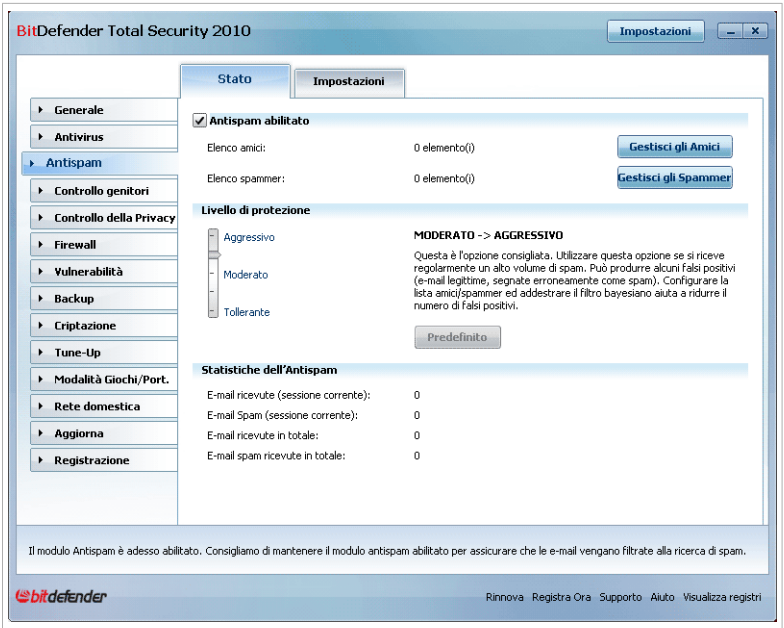
- nuove impronte di immagini saranno aggiunte al **Filtro Immagine**.
- nuovi links verranno aggiunti al **Filtro URL**.
- nuove regole verranno aggiunte al **Filtro Euristico**.

Questo aiuterà ad incrementare l'effettività del tuo motore Antispam.

Per proteggerti contro gli spammers, BitDefender può effettuareaggiornamenti automatici. Mantenere l'opzione di **Aggiornamento Automatico** attivata.

19.2. Stato

Per configurare la protezione Antispam, fare clic su **Antispam>Stato** in Modalità Avanzata.



Stato dell'Antispam

Potete vedere se l'Antispam è abilitato o disabilitato. Se desiderate cambiare lo stato dell'Antispam, deselezionare o selezionare la casella corrispondente.

Importante
Per impedire che lo Spam entri nella vostra **Inbox**, mantenere abilitato il **Antispam filter**.

Nella sezione **Statistiche** è possibile visionare i risultati della attività dell'Antispam presentati per sessione (da quando avete avviato il computer), oppure un riassunto (dall'installazione di BitDefender).

19.2.1. Impostazione del Livello di Protezione

Potete scegliere il livello di protezione che meglio si adatta alle vostre necessità di sicurezza. Trascinate il pulsante sulla barra per impostare il livello di protezione appropriato.

Ci sono 5 livelli di protezione:

Livello di protezione	Descrizione
Permissiva	Offre protezione per gli account che ricevono molta posta commerciale legittima. Il filtro lasciare passare la maggior parte delle e-mail, ma potrebbe produrre dei falsi negativi (spam classificato come mail legittime).
Permissivo a Moderato	Offre protezione per account che ricevono alcune mail commerciali legittime. Il filtro lasciare passare la maggior parte delle e-mail, ma potrebbe produrre dei falsi negativi (spam classificato come mail legittime).
Moderato	Offre protezione per account normali. Il filtro bloccherà la maggior parte dello spam, evitando al contempo i falsi positivi.
Da Moderato ad Aggressivo	Offre protezione per gli account che ricevono regolarmente ampi volumi di spam. Il filtro lascerà passare pochissimo spam, ma potrebbe produrre dei falsi positivi (mail legittime etichettate erroneamente come spam). Configura gli **Elenchi Amici/Spammer** e addestra il **Motore di Apprendimento (Bayesiano)** per ridurre il numero di falsi positivi.
Aggressiva	Offre protezione per gli account che ricevono regolarmente volumi di spam molto ampi. Il filtro lascerà passare pochissimo spam, ma potrebbe produrre dei falsi positivi (mail legittime etichettate erroneamente come spam). Aggiungete i vostri contatti alla **Lista Amici** per ridurre il numero di falsi positivi.

Per impostare il livello di protezine di default (**Da Moderato ad Aggressivo**) cliccare su **Livello di Default**.

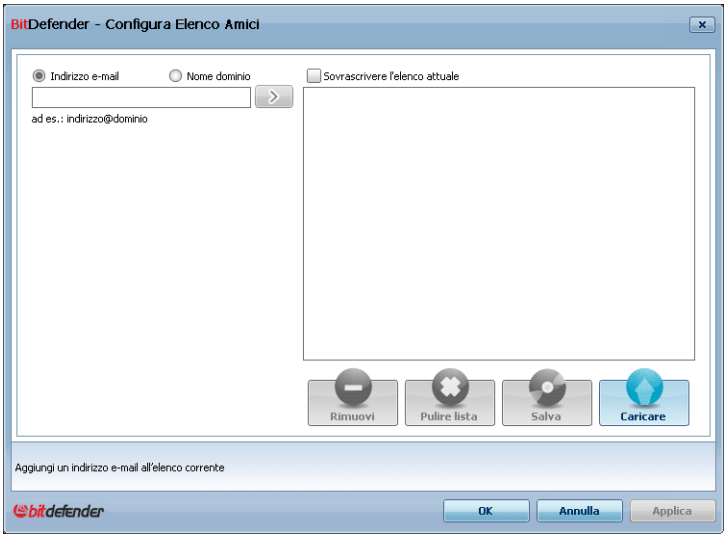
19.2.2. Configurazione dell'Elenco Amici

L'**Elenco Amici** è l'elenco di tutti gli indirizzi email dai quali volete sempre ricevere messaggi, indipendentemente dal loro contenuto. I messaggi provenienti dai vostri amici non verranno etichettati come spam, anche se il loro contenuto potrebbe assomigliare allo Spam.

Nota

Qualsiasi mail in arrivo da un indirizzo contenuto nella lista **Elenco Amici**, sarà automaticamente consegnato alla vostra Inbox senza alcun ulteriore processo.

Per configurare l'Elenco Amici, fare clic su **Gestione Amici** (oppure fare clic sul pulsante **Amici** nella barra degli strumenti Antispam).



Elenco Amici

Qui potrete aggiungere o rimuovere elementi dall'**Elenco Amici**.

Se si desidera aggiungere un indirizzo email, selezionare il campo **Indirizzo E-mail**, inserire l'indirizzo e premere il pulsante . L'indirizzo apparirà nell'**Elenco amici**.

Importante
Sintassi: name@domain.com.

Se desiderate aggiungere un dominio, selezionare l' opzione **Dominio**, digitare dominio e premere il pulsante . Il dominio apparirà sull'**Elenco Amici**.

Importante
Sintassi:

- @domain.com, *domain.com e domain.com - tutte le mail provenienti da domain.com raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;
- *domain* - tutte le mail provenienti da domain (non importa il suffisso del dominio) raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;
- *com - tutte le mail con il suffisso di dominio com raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;

Per rimuovere un elemento dall'elenco, selezionarlo e fare clic su **Rimuovi**. Per eliminare tutti gli elementi dall'elenco fare clic su **Pulisci elenco** e quindi su **Sì** per confermare.

E' possibile salvare l'elenco Amici in un file in modo da poterlo riutilizzare su un altro computer o dopo aver reinstallato il prodotto. Per salvare l'elenco Amici, fare clic sul pulsante **Salva** e salvare nella posizione desiderata. Il file avrà estensione `.bwl`.

Per caricare un elenco Amici precedentemente salvato, fare clic sul pulsante **Carica** e aprire il corrispondente file `.bwl`. Per ripristinare il contenuto dell'elenco esistente quando si carica un elenco precedentemente salvato, selezionare **Sovrascrivi l'elenco attuale**.

Nota

Raccomandiamo di aggiungere i nomi dei vostri amici e gli indirizzi e-mail all'**elenco Amici**. BitDefender non blocca i messaggi di coloro che sono nell'elenco; aggiungere amici aiuta a garantire che i messaggi leciti vengano recapitati.

Selezionare **Applica** e **OK** per salvare & chiudere **l'Elenco Amici**.

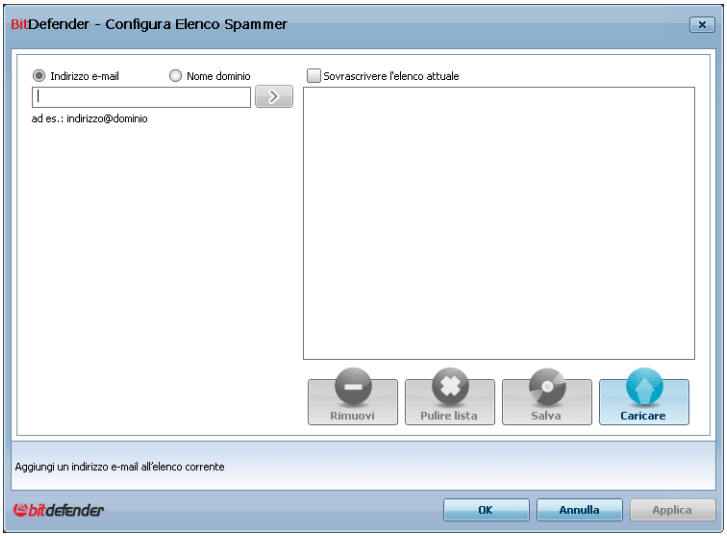
19.2.3. Configurazione dell'Elenco Spammer

L'**Elenco Spammer** è l'elenco di tutti gli indirizzi e-mail dai quali non volete ricevere messaggi, indipendentemente dal loro contenuto.

Nota

Qualsiasi mail in arrivo da un indirizzo contenuto nell'**Elenco Spammer** verrà automaticamente marcato come Spam, senza alcun ulteriore processo.

Per configurare l'Elenco Spammer, fare clic su **Gestione Spammer** (oppure fare clic sul pulsante **Spammer** nella barra degli strumenti Antispam).



Elenco Spammers

Qui potrete aggiungere o rimuovere elementi dall'**Elenco Spammer**.

Se desiderate aggiungere un indirizzo email, selezionare il campo **Indirizzo Email**, inserire l'indirizzo e premere il pulsante . L'indirizzo apparirà nell'**Elenco Spammers**.

Importante
Sintassi: name@domain.com.

Se volete aggiungere un dominio, selezionare l'opzione **Dominio**, digitare il nome e fare un click su . Il dominio apparirà nell'**Elenco Spammers**.

Importante
Sintassi:

- @domain.com, *domain.com e domain.com - tutte le mail provenienti da domain.com verranno marcate come Spam;
- *domain* - tutte le mail provenienti da domain (indipendentemente dai suffissi del dominio) verranno marcate come Spam;
- *com - tutte le mail con il suffisso di dominio com verranno marcate come Spam.

Avvertimento

Non aggiungere domini di servizi e-mail legittimi (ad esempio Yahoo, Gmail, Hotmail o altri) all'elenco Spammer. In caso contrario gli indirizzi e-mail ricevuti dagli utenti registrati di tali servizi verranno identificati come spam. Se ad esempio si aggiunge `yahoo.com` all'elenco Spammer, tutti i messaggi e-mail provenienti da indirizzi `yahoo.com` saranno contrassegnati come `[spam]`.

Per rimuovere un elemento dall'elenco, selezionarlo e fare clic su **Rimuovi**. Per eliminare tutti gli elementi dall'elenco fare clic su **Pulisci elenco** e quindi su **Sì** per confermare.

E' possibile salvare l'elenco Spammer in un file in modo da poterlo riutilizzare su un altro computer o dopo aver reinstallato il prodotto. Per salvare l'elenco Spammer, fare clic sul pulsante **Salva** e salvare nella posizione desiderata. Il file avrà estensione `.bwl`.

Per caricare un elenco Spammer precedentemente salvato, fare clic sul pulsante **Carica** e aprire il corrispondente file `.bwl`. Per ripristinare il contenuto dell'elenco esistente quando si carica un elenco precedentemente salvato, selezionare **Sovrascrivi l'elenco attuale**.

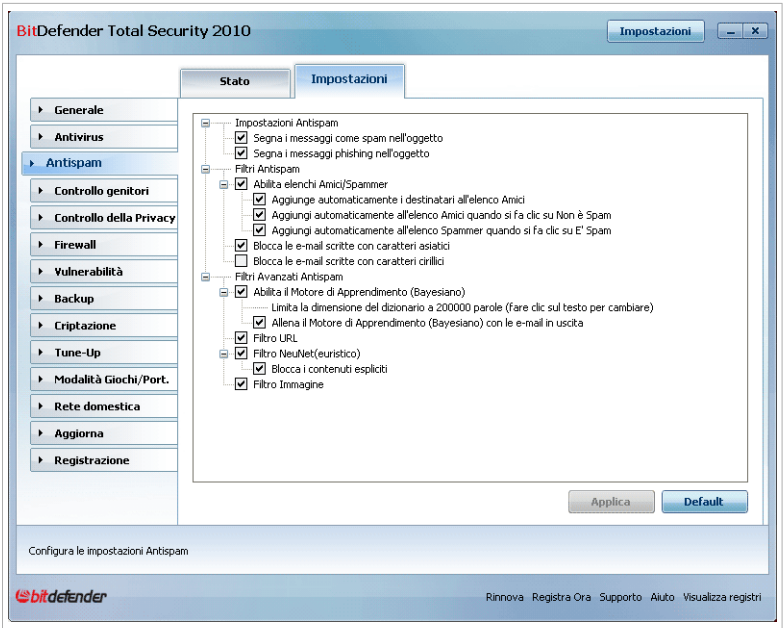
Selezionare **Applica** e **OK** tper salvare & chiudere **l'Elenco Spammer**.

Importante

Se si desidera installare nuovamente BitDefender, consigliamo prima di salvare gli elenchi **Amici** / **Spammer** e di ricaricarli al termine del processo di re-installazione.

19.3. Impostazioni

Per configurare le impostazioni ed i filtri antispam, fare clic su **Antispam>Impostazioni** in Modalità Avanzata.



Impostazioni Antispam

Sono disponibili tre categorie di opzioni (**Impostazioni Antispam**, **Filtri Antispam** and **Filtri Avanzati Antispam**) organizzati come menu espandibili, simili a quelli di Windows.

Nota
Selezionare una casella con "+" per aprire una categoria oppure una casella con "-" per chiudere una categoria.

Per attivare/disattivare una opzione, selezionare/pulire il checkbox corrispondente.

Per applicare le impostazioni predefinite, cliccare su **Default**.

Click **Applica** per salvare le modifiche.

19.3.1. Impostazioni Antispam

- **Contrassegna i messagi spam nel soggetto** - tutti i messaggi email considerati come Spam verranno marcati con Spam nel soggetto.
- **Marca l'oggetto dei messagi considerati come phishing** - tutte le mail considerate messaggi di phishing saranno etichettate come SPAM sulla linea di Oggetto.

19.3.2. Filtri Antispam

- **Abilita elenchi Amici / Spammer** - filtra i messaggi e-mail utilizzando gli Elenchi Amici/Spammer.
  - **Aggiungi automaticamente all'elenco degli Amici** - aggiunge automaticamente i mittenti all'Elenco Amici.
  - **Aggiungi Automaticamente all'Elenco Amici** - quando verrà premuto il pulsante **Non è Spam** dalla Barra degli strumenti Antispam, il mittente della e-mail selezionata verrà aggiunto automaticamente all'Elenco Amici.
  - **Aggiungi automaticamente all'elenco Spammer** - quando verrà premuto il pulsante **È Spam** dalla Barra degli strumenti Antispam il mittente della e-mail selezionata verrà automaticamente aggiunto all'Elenco Spammer.

Nota
I tasti **Non è Spam** ed **è Spam** vengono utilizzati per "istruire" il Filtro bayesiano.

- **Bloccare messaggi e-mail scritti in caratteri asiatici** - blocca i messaggi scritti in Caratteri Asiatici.
- **Bloccare messaggi e-mail scritti in caratteri cirillici** - blocca i messaggi scritti in Caratteri cirillici.

19.3.3. Filtri Avanzati Antispam

- **Abilita il motore di Apprendimento (bayesiano)** - attiva/disattiva il Motore di Apprendimento (bayesiano).
  - **Limita la dimensione del vocabolario a 200000 parole** - con questa opzione potete impostare la dimensione del dizionario Bayesiano – se minore è più veloce, se maggiore è più accurato.

Nota
La dimensione consigliata è: 200.000 parole.

  - **Istruisci il Motore di Apprendimento (bayesiano) per le e-mails in uscita** - istruisce il Motore di Apprendimento (bayesiano) per le e-mail in uscita.
- **Filtro URL** - attiva/disattiva il Filtro URL;
- **Filtro Euristico** - attiva/disattiva il Filtro Euristico;
  - **Blocco dei contenuti espliciti** - attiva/disattiva la scansione di messaggi "SESSUALMENTE ESPLICITO" nell'oggetto.
- **Filtro immagini** - attivare/disattivare il Filtro immagini.

20. Controllo genitori

Il Controllo dei Genitori BitDefender vi permette di controllare l'accesso ad Internet e ad applicazioni specifiche di ogni utente che possieda un account nel sistema.

Potete configurare il Controllo dei Genitori per bloccare:

- pagine web inappropriate.
- accesso ad Internet, durante specifici periodi di tempo (come durante le ore di studio).
- pagine web, e-mail e messaggi istantanei contenenti determinate parole.
- applicazioni come giochi, chat, programmi di condivisione di file ed altri.
- messaggi istantanei inviati da contatti chat diversi da quelli consentiti.

Importante

Solo gli utenti con diritti di amministrazione (amministratori del sistema) possono accedere e configurare il Controllo dei Genitori. Per essere sicuri che solo voi potrete modificare le impostazioni del Controllo dei Genitori per qualsiasi utente, potete proteggerle mediante una password. Vi verrà chiesto di configurare la password quando abiliterete il Controllo dei Genitori per un utente specifico.

Per utilizzare con successo il Controllo dei Genitori e limitare l'uso del computer e le attività online dei vostri bambini, dovete completare questi task:

1. Creare degli account di Windows limitati (standard) per i bambini.

Nota

Per imparare a creare account di Windows, fare clic su Guida in linea e Supporto tecnico di Windows (nel menu Start, fare clic su **Guida in linea e Supporto tecnico**).

2. Configurare il Controllo dei Genitori per gli account di Windows che verranno usati dai vostri bambini.

Per configurare il Controllo Genitori, fare clic su **Controllo Genitori** in Modalità Avanzata.

Controllo genitori

E' possibile visualizzare le informazioni relative allo stato del Controllo Genitori per ogni account utente di Windows. La categoria di età è elencata al di sotto di ciascun nome utente se il Controllo Genitori è abilitato. Se il Controllo Genitori è disabilitato, lo stato è **non configurato**.

Inoltre è possibile visualizzare lo stato di ciascuna caratteristica del Controllo Genitori per utente:

Cerchio verde con un segno di spunta: La caratteristica è abilitata.
Cerchio rosso con un punto esclamativo: La caratteristica è disabilitata.

Fare clic sul pulsante **Modifica** vicino ad un nome utente per aprire la finestra in cui è possibile configurare il Controllo Genitori per l'account utente corrispondente.

Le seguenti sezioni di questo capitolo presentano in dettaglio le funzioni del Controllo dei Genitori e come configurarle.

20.1. Configurazione del Controllo Genitori per un utente

Per configurare il Controllo Genitori per uno specifico account utente fare clic sul pulsante **Modifica** corrispondente a tale account utente e quindi fare clic sulla scheda **Stato**.

Stato del Controllo Genitori

Per configurare il Controllo dei Genitori per questo account, seguire questi passaggi:

1. Abilitare il Controllo Genitori per questo account utente selezionando la casella di controllo **Controllo Genitori**.

   Importante
   Mantenere il **Controllo dei Genitori** abilitato per proteggere i vostri bambini dai contenuti inopportuni utilizzando le vostre regole di accesso al computer personalizzate.

2. Impostare una password per proteggere le vostre impostazioni del Controllo dei Genitori. Per ulteriori informazioni, vi preghiamo di riferirvi a «*Protezione delle Impostazioni del Controllo dei Genitori*» (p. 225).
3. Impostare la categoria di età per permettere ai bambini di accedere solo ai siti web appropriati per la loro età. Per ulteriori informazioni fare riferimento a «*Impostazione della Categoria di Età*» (p. 226).
4. Configurare le opzioni di controllo per questo utente come necessario:
   - **Invia un rapporto attività via e-mail.** Viene inviata una notifica e-mail ogni volta che il Controllo Genitori di BitDefender blocca un'attività di questo utente.
   - **Salva un registro del traffico Internet.** Registra i siti web visitati dall'utente.

Per ulteriori informazioni fare riferimento a *«Controllo Attività dei Bambini»* (p. 229).

5. Fare clic su un'icona o una scheda per configurare la caratteristica di Controllo Genitori corrispondente:
   - **Web** - per filtrare la navigazione sul web secondo le regole impostate nella sezione Web.
   - **Applicazioni** per bloccare l'accesso alle applicazioni specificate nella sezione Applicazioni.
   - **Parole Chiave** - per filtrare l'accesso al web, alla posta ed all'instant messaging secondo le regole impostate nella sezione Parole Chiave.
   - **IM** - per consentire o impedire le chat con i contatti di instant messaging secondo le regole impostate nella sezione Traffico IM.
   - **Limitatore di Tempo** - per consentire l'accesso al web secondo l'orario stabilito nella sezione Limitatore di Tempo.

   Nota

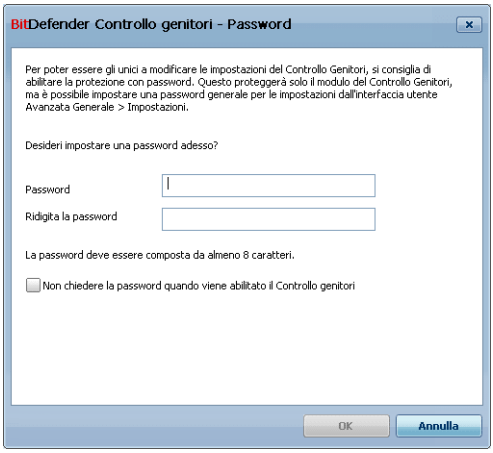
   Per imparare a configurarle, vi preghiamo di riferirvi ai seguenti argomenti in questo capitolo.

Per bloccare completamente l'accesso ad internet, fare clic sul pulsante **Blocca Internet**.

20.1.1. Protezione delle Impostazioni del Controllo dei Genitori

Se non siete l'unica persona ad utilizzare questo computer con diritti di amministratore, consigliamo di proteggere le vostre Impostazioni del Controllo dei Genitori con una password. Impostando una password, impedirete ad altri utenti con diritti di amministratore di modificare le impostazioni del Controllo dei Genitori che avete configurato per un utente specifico.

BitDefender vi chiederà di default di impostare una password quando abiliterete il Controllo dei Genitori.


BitDefender Controllo genitori - Password
Per poter essere gli unici a modificare le impostazioni del Controllo Genitori, si consiglia di abilitare la protezione con password. Questo proteggerà solo il modulo del Controllo Genitori, ma è possibile impostare una password generale per le impostazioni dall'interfaccia utente Avanzata Generale > Impostazioni.
Desideri impostare una password adesso?
Password
Ridigita la password
La password deve essere composta da almeno 8 caratteri.
Non chiedere la password quando viene abilitato il Controllo genitori
OK
Annulla

Imposta Protezione password

Per impostare la protezione mediante password, fare come segue:

1. Digitare la password nel campo **Password**.
2. Digitare di nuovo la password nel campo **Ridigitare Password** per confermarla.
3. Selezionare **OK** per salvare la password e chiudere la finestra.

Una volta impostata la password, se desiderate modificare le impostazioni del Controllo dei Genitori, vi verrà richiesta la password. Gli altri amministratori del sistema (se ci fossero) dovranno anche fornire la password per potere modificare le impostazioni del Controllo dei Genitori.

Nota
Questa password non proteggerà altre impostazioni di BitDefender.

Nel caso in cui non impostate una password e non volete che questa finestra compaia di nuovo, selezionare **Non chiedere password all'abilitazione del Controllo dei Genitori**.

20.1.2. Impostazione della Categoria di Età

Il Filtro Euristico Web analizza le pagine web e blocca quelle che corrispondono a modelli dal contenuto potenzialmente inappropriato.

Per filtrare l'accesso al web secondo regole predefinite basate sull'età, dovrete impostare un livello specifico di tolleranza. Trascinate il pulsante scorrevole lungo

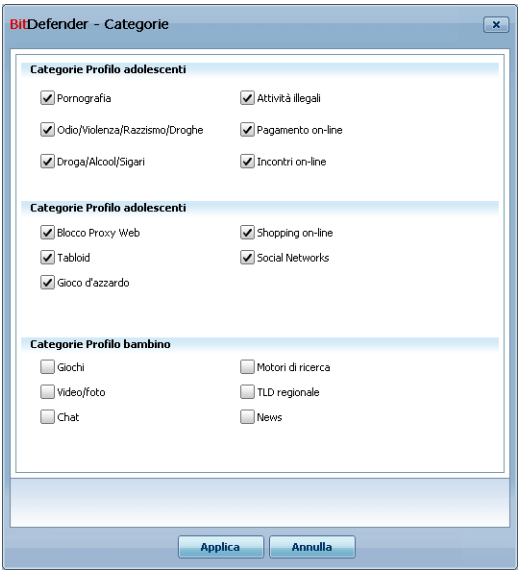
la barra per impostare il livello di tolleranza che considerate appropriato per l'utente selezionato.

Ci sono 3 livelli di tolleranza:

Livello di tolleranza	Descrizione
Bambino	Offre un accesso web limitato, secondo le impostazioni raccomandate per gli utenti al di sotto dei 14 anni. Le pagine web con contenuto potenzialmente dannoso per i bambini (porno, sessualità, droghe, hacking ecc.) sono bloccate.
Adolescenti	Offre un accesso web limitato, secondo le impostazioni raccomandate per gli utenti con età tra i 14 e i 18 anni. Le pagine web con contenuto sessuale, pornografico o per adulti sono bloccate.
Adulti	Offre un accesso illimitato a tutte le pagine web indipendentemente dal loro contenuto.

Cliccare su **Livello di Default** per impostare il pulsante scorrevole al livello di default.

Se si desidera avere maggior controllo sul tipo di contenuto a cui l'utente è esposto su Internet, è possibile definire le categorie di contenuto web che verranno bloccate dal filtro web. Per selezionare che tipi di contenuto web si desidera bloccare, fare clic su **Categorie Personalizzate**. Apparirà una nuova finestra:



Categorie Filtri Web

Selezionare la casella di controllo corrispondente alla categoria che si desidera bloccare e all'utente non sarà più permesso l'accesso ai siti web corrispondenti a tale categoria. Per rendere la selezione più semplice, le categorie di contenuto web sono elencate in base al gruppo di età per cui potrebbero essere considerate appropriate:

- **Categorie Profilo Bambino** include contenuti a cui è consentito l'accesso a bambini al di sotto dei 14 anni.

Categoria	Descrizione
Giochi	Siti web che offrono giochi da browser, forum di discussione sui giochi, download di giochi, trucchi, soluzioni, ecc.
Video/Foto	Website che ospitano gallerie di video o foto.
IM	Applicazioni di messaggistica istantanea.
Motori di Ricerca	Motori e portali di ricerca.
TLD Regionale	Siti web il cui nome di dominio è al di fuori della regione dell'utente.
Notizie	Giornali on-line.

- **Categorie Profilo Adolescenti** include contenuti che possono essere considerati sicuri per bambini fra i 14 e i 18 anni di età.

Categoria	Descrizione
Blocco Proxy Web	Siti web utilizzati per mascherare l'URL di un sito web richiesto.
Tabloid	Riviste on-line.
Gioco d'Azzardo	Casino on-line, siti web di scommesse, siti che offrono consigli sulle scommesse, forum sulle scommesse, ecc.
Shopping Online	Negozi e boutique on-line.
Social Network	Siti web di Social Networking.

- **Categorie Profilo Adulto** include contenuti non adatti ai bambini o agli adolescenti.

Categoria	Descrizione
Pornografia	Siti web con contenuto pornografico.
Odio / Violenza / Razzismo / Droghe	Siti web con contenuto violento o razzista, che promuovono il terrorismo o l'utilizzo di droghe.
Medicinali / Alcool / Sigari	Siti web che vendono o pubblicizzano medicinali, alcool o prodotti a base di tabacco.
Attività Illegali	Siti web che promuovono la pirateria od ospitano contenuti pirata.
Pagamenti On-line	Moduli web per i pagamenti on-line e sezioni di pagamento dei negozi on-line. L'utente può visitare i negozi on-line ma i tentativi di acquisto vengono bloccati.
Appuntamenti On-line	Siti web per appuntamenti per adulti, con chat, video o scambio di foto.

Fare clic su **Applica** per salvare le categorie di contenuto web bloccato per l'utente.

20.2. Controllo Attività dei Bambini

BitDefender permette di controllare ciò che fanno i vostri figli al computer anche quando non siete presenti. Possono essere inviati avvisi via e-mail ogni volta che il modulo Controllo Genitori blocca un'attività. Inoltre è possibile salvare un registro con la cronologia dei siti visitati.

Selezionare le opzioni che si desidera abilitare:

- **Invia un rapporto attività via e-mail.** Viene inviata una notifica e-mail ogni volta che il Controllo Genitori di BitDefender blocca un'attività.
- **Salva un registro del traffico Internet.** Registra i siti web visitati dagli utenti per cui è abilitato il Controllo Genitori.

20.2.1. Controllo dei Siti Web visitati

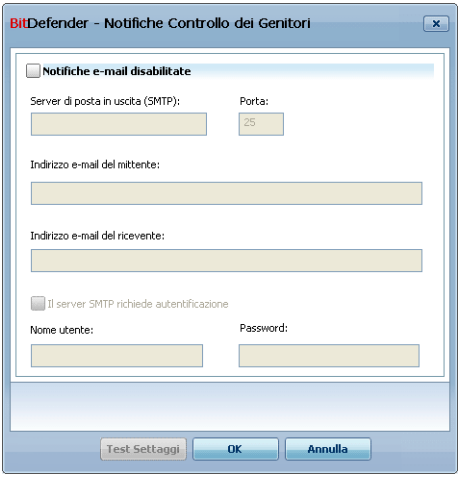
BitDefender registra per default i siti web visitati dai bambini.

Per visualizzare i registri fare clic su **Visualizza Registri** per aprire Cronologia&Eventi e selezionare **Registro Internet**.

20.2.2. Configurazione Notifiche E-mail

Per ricevere notifiche via e-mail quando il Controllo Genitori blocca un'attività, selezionare **Invia un rapporto attività via e-mail** nella finestra di configurazione generale del Controllo Genitori. Verrà richiesto di configurare le impostazioni dell'account e-mail. Fare clic su **Sì** per aprire la finestra di configurazione.

Nota
E' possibile aprire la finestra di configurazione in un secondo momento facendo clic su **Impostazioni Notifiche**.



Impostazioni E-mail

Le impostazioni dell'account e-mail devono essere configurate come segue:

- **Server SMTP in Uscita** - digitare l'indirizzo del server di posta utilizzato per inviare i messaggi e-mail.
- Se il server usa una porta diversa rispetto alla porta di default 25, digitare il numero della porta nel campo corrispondente.
- **Indirizzo e-mail mittente** - digitare l'indirizzo che si vuole che appaia nel campo **Da** dell'e-mail.
- **Indirizzo e-mail destinatario** - digitare l'indirizzo a cui si desidera inviare i rapporti.
- Se il server richiede l'autenticazione, selezionare la casella di controllo **Il mio server SMTP richiede l'autenticazione** e digitare il nome utente e la password nei campi corrispondenti.

Nota

Se non si conoscono tali impostazioni apprire l'applicazione usata per la posta e controllare le impostazioni dell'account e-mail.

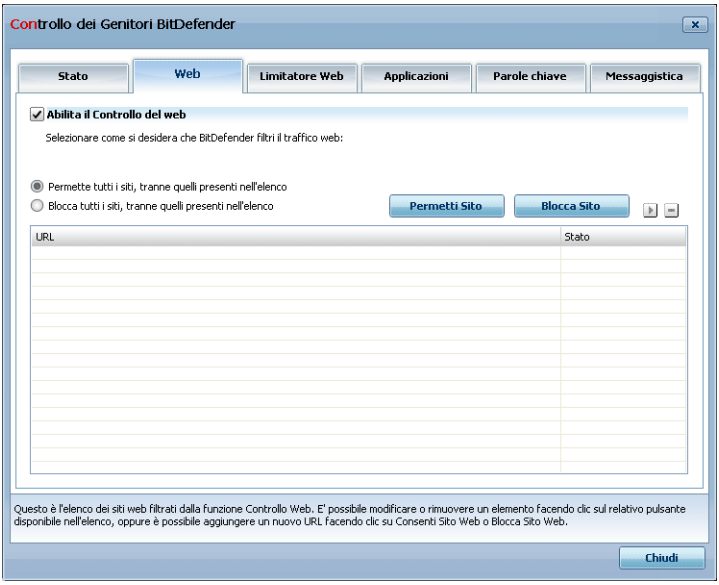
Per convalidare la configurazione, fare clic sul pulsante **Verifica Impostazioni**. Se vengono identificati dei problemi durante la convalida, BitDefender comunicherà quali aree necessitano della vostra attenzione.

Selezionare **OK** per salvare le modifiche e chiudere la finestra.

20.3. Controllo Web

Il **Controllo Web** vi aiuta a bloccare l'accesso ai siti web inappropriati. Una lista di utenti per bloccare sia i siti inappropriati che parte di essi é fornita e aggiornata da BitDefender come parte del processo di aggiornamento regolare.

Per configurare il Controllo Web per uno specifico account utente fare clic sul pulsante **Modifica** corrispondente a tale account utente e quindi fare clic sulla scheda **Web**.


Controllo dei Genitori BitDefender
Stato
Web
Limitatore Web
Applicazioni
Parole chiave
Messaggistica
Abilita il Controllo del web
Selezionare come si desidera che BitDefender filtri il traffico web:
Permette tutti i siti, tranne quelli presenti nell'elenco
Blocca tutti i siti, tranne quelli presenti nell'elenco
Permetti Sito
Blocca Sito
URL
Stato
Questo è l'elenco dei siti web filtrati dalla funzione Controllo Web. E' possibile modificare o rimuovere un elemento facendo clic sul relativo pulsante disponibile nell'elenco, oppure è possibile aggiungere un nuovo URL facendo clic su Consenti Sito Web o Blocca Sito Web.
Chiudi

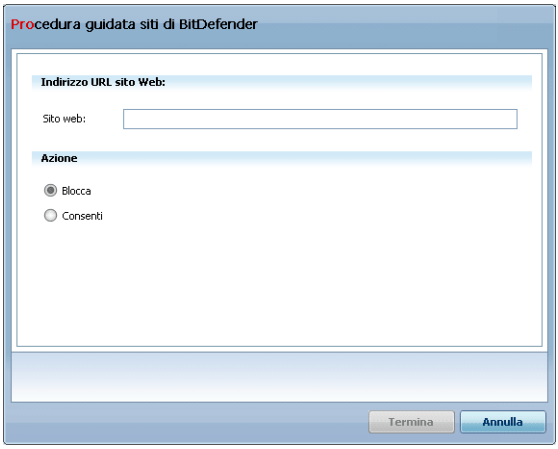
Controllo Web

Per abilitare questa protezione selezionare la casella di controllo che corrisponde a **Abilita il Controllo Web**.

20.3.1. Creazione Regole di Controllo Web

Per permettere o bloccare l'accesso ad un sito web seguire questi passi:

1. Fare clic su **Permetti Sito** oppure su **Blocca Sito**. Apparirà una nuova finestra:



Specificare i siti web

2. Inserire l'URL del sito web nel campo **Sito web**.
3. Selezionare l'azione desiderata per questa regola - **Permetti** oppure **Blocca**.
4. Cliccare su**OK** per aggiungere la regola.

20.3.2. Gestione delle Regole di Controllo Web

Le regole di Controllo Web configurate sono elencate in una tabella nella parte inferiore della finestra. Per ogni regola del Controllo Web sono elencati l'indirizzo del sito web e lo stato attuale.

Per modificare una regola, selezionarla e fare clic sul pulsante **Modifica** e quindi eseguire le modifiche necessarie nella finestra di configurazione. Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina**.

È anche necessario selezionare quale azione verrà intrapresa da Controllo Genitori di Bitdefender per i siti web per cui non esistono regole di Controllo Web:

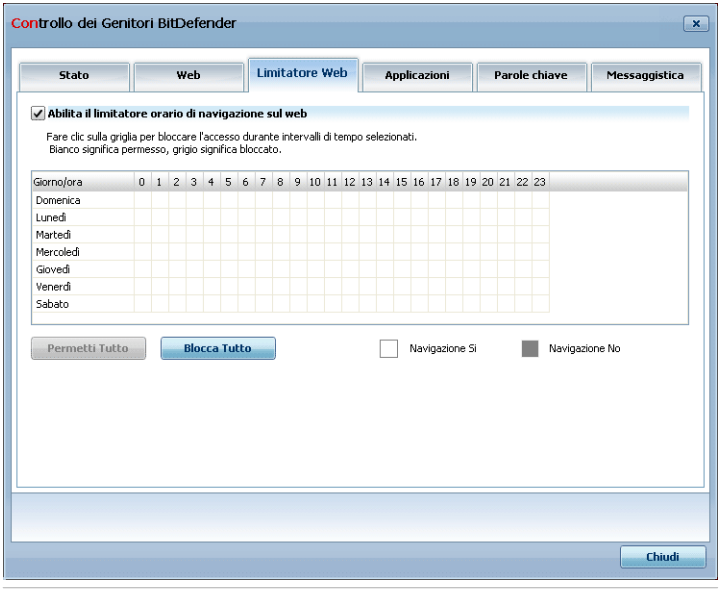
- **Permetti tutti i siti, tranne quelli nell'elenco**. Selezionare questa opzione per permettere l'accesso a tutti i siti web eccetto quelli per cui è stata impostata l'azione **Blocca**.
- **Blocca tutti i siti, tranne quelli nell'elenco**. Selezionare questa opzione per bloccare l'accesso a tutti i siti web eccetto quelli per cui è stata impostata l'azione **Permetti**.

20.4. Limitatore di Tempo su Web

Il **Tempo limitato sul web** ti aiuta a bloccare l'accesso a internet per determinati periodi di tempo.

Nota
BitDefender eseguirà aggiornamenti ogni ora indipendentemente dall'impostazione **Tempo limitato sul web**.

Per configurare il Limitatore di Orario Web per uno specifico account utente fare clic sul pulsante **Modifica** corrispondente a tale account utente e quindi fare clic sulla scheda **Limitatore Web**.



Limitatore di Tempo su Web

Per abilitare questa protezione seleziona la casella di controllo che corrisponde a **Abilita Tempo limitato sul web**.

Selezionare gli intervalli di tempo in cui tutti i collegamenti a Internet verranno bloccati. È possibile fare clic sulle celle individuali oppure fare clic e trascinare per coprire periodi di tempo più lunghi. Inoltre è anche possibile fare clic su **Blocca tutto** per selezionare tutte le celle e implicitamente bloccare completamente l'accesso web. Se si fa clic su **Permetti tutto**, le connessioni Internet saranno sempre permesse.

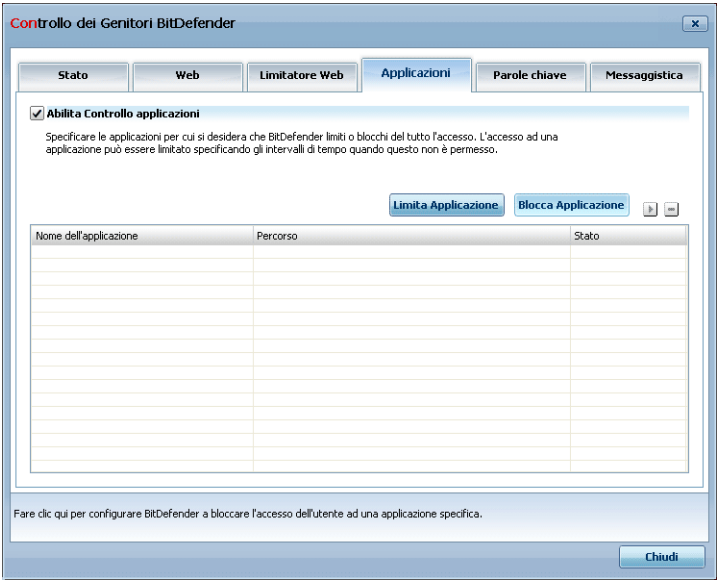
Importante

I box colorati in grigio rappresentano l'intervallo di tempo quando la connessione internet è bloccata.

20.5. Controllo applicazioni

Il **Controllo Applicazioni** ti aiuta a bloccare qualsiasi applicazione in esecuzione. Giochi, messaggi software, oltre ad altre categorie di software e minacce che in questo caso possono essere bloccati. Le applicazioni bloccate sono così protette da modifiche, e non possono essere copiate o spostate. È possibile bloccare le applicazioni permanentemente o solo per determinati periodi di tempo, ad esempio quando i vostri bambini dovrebbero fare i compiti.

Per configurare il Controllo Applicazioni per uno specifico account utente fare clic sul pulsante **Modifica** corrispondente a tale account utente e quindi fare clic sulla scheda **Applicazioni**.


Controllo dei Genitori BitDefender
Stato
Web
Limitatore Web
Applicazioni
Parole chiave
Messaggistica
Abilita Controllo applicazioni
Specificare le applicazioni per cui si desidera che BitDefender limiti o blocchi del tutto l'accesso. L'accesso ad una applicazione può essere limitato specificando gli intervalli di tempo quando questo non è permesso.
Limita Applicazione
Blocca Applicazione
Nome dell'applicazione
Percorso
Stato
Fare clic qui per configurare BitDefender a bloccare l'accesso dell'utente ad una applicazione specifica.
Chiudi

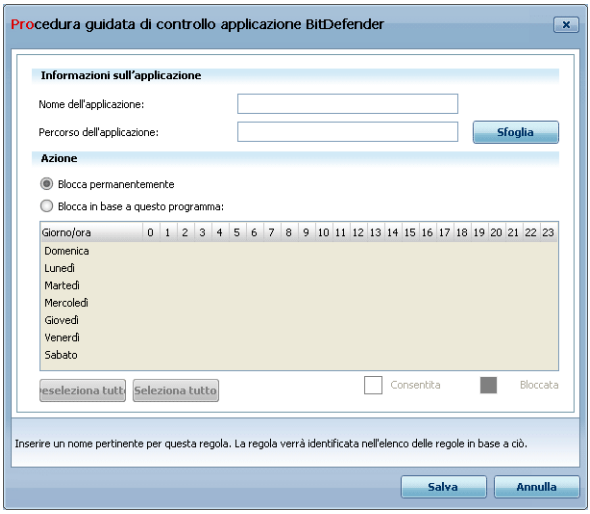
Controllo applicazioni

Per abilitare questa protezione selezionare la casella di controllo che corrisponde a **Abilita Controllo Applicazioni**.

20.5.1. Creazione Regole di Controllo Applicazioni

Per bloccare o limitare l'accesso ad un'applicazione seguire questi passi:

1. Fare clic su **Blocca Applicazione** oppure su **Restringi Applicazione**. Apparirà una nuova finestra:



Specificare l'applicazione

2. Fare clic su **Sfoglia** per localizzare l'applicazione di cui si desidera bloccare/restringere l'accesso.
3. Selezionare l'azione della regola:
   - **Blocca permanentemente** per bloccare completamente l'accesso all'applicazione.
   - **Blocca in base ad un programma** per limitare l'accesso a determinati intervalli di tempo.

   Se si sceglie di restringere l'accesso piuttosto che bloccare completamente l'applicazione, è anche necessario selezionare dalla griglia i giorni e gli intervalli di tempo durante i quali l'accesso è bloccato. È possibile fare clic sulle celle individuali oppure fare clic e trascinare per coprire periodi di tempo più lunghi. Inoltre è anche possibile fare clic su **Seleziona tutto** per selezionare tutte le celle e implicitamente bloccare completamente l'applicazione. Se si fa clic su **Deseleziona tutto**, l'accesso all'applicazione sarà permesso in ogni momento.
4. Cliccare su**OK** per aggiungere la regola.

20.5.2. Gestione Regole di Controllo Applicazioni

Le regole di Controllo Applicazioni che sono state configurate sono elencate in una tabella nella parte inferiore della finestra. Per ogni regola di Controllo Applicazioni viene elencato il nome dell'applicazione, il percorso e lo stato attuale.

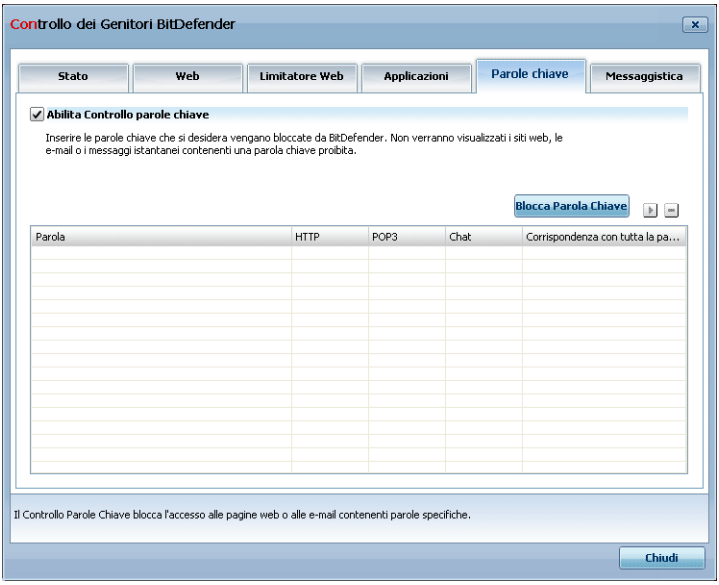
Per modificare una regola, selezionarla e fare clic sul pulsante **Modifica** e quindi eseguire le modifiche necessarie nella finestra di configurazione. Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina**.

20.6. Controllo parole chiave

Il Controllo Parole Chiave aiuta a bloccare l'accesso degli utenti a messaggi e-mail, pagine web e messaggi istantanei che contengano parole specifiche. Utilizzando il Controllo Parole Chiave è possibile impedire ai bambini di vedere parole o frasi inappropriate quando sono online.

Nota
Il Controllo Parole Chiave per la messaggistica istantanea è disponibile solo per Yahoo Messenger e Windows Live (MSN) Messenger.

Per configurare il Controllo Parole Chiave per uno specifico account utente fare clic sul pulsante **Modifica** corrispondente a tale account utente e quindi fare clic sulla scheda **Parole Chiave**.


Controllo dei Genitori BitDefender
Stato
Web
Limitatore Web
Applicazioni
Parole chiave
Messaggistica
Abilita Controllo parole chiave
Inserire le parole chiave che si desidera vengano bloccate da BitDefender. Non verranno visualizzati i siti web, le e-mail o i messaggi istantanei contenenti una parola chiave proibita.
Blocca Parola Chiave
Parola
HTTP
POP3
Chat
Corrispondenza con tutta la pa...
Il Controllo Parole Chiave blocca l'accesso alle pagine web o alle e-mail contenenti parole specifiche.
Chiudi

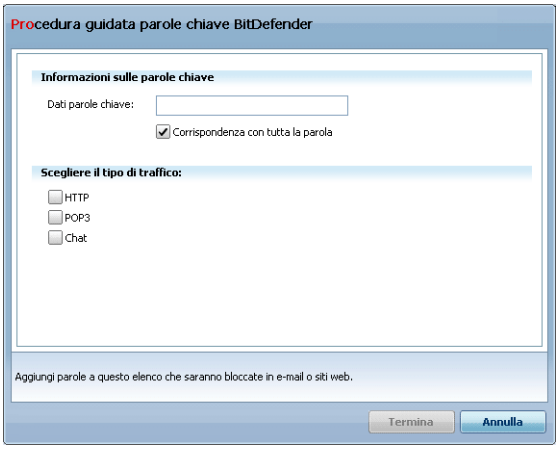
Controllo parole chiave

Selezionare la casella di controllo **Abilita Controllo Parole Chiave** se si desidera usare questa funzione di controllo.

20.6.1. Creazione Regole di Controllo Parole Chiave

Per bloccare una parola o una frase è necessario seguire questi passi:

1. Fare clic su **Blocca Parola Chiave**. Apparirà una nuova finestra:



Specificare Parole Chiave

2. Digitare la parola o frase che si desidera bloccare nel campo di immissione. Se si desidera che vengano rilevate solo parole intere, selezionare la casella di controllo **Solo parole intere**.
3. Selezionare il tipo di traffico che BitDefender dovrà analizzare alla ricerca della parola specificata.

Opzione	Descrizione
HTTP	Le pagine web che contengono la parola chiave sono bloccate.
POP3	I messaggi e-mail che contengono la parola chiave sono bloccati.
Instant Messaging	I messaggi istantanei che contengono la parola chiave sono bloccati.

4. Cliccare su**OK** per aggiungere la regola.

20.6.2. Gestione delle Regole di Controllo Parole Chiave

Le regole di Controllo Parole Chiave che sono state configurate sono elencate in una tabella nella parte inferiore della finestra. Per ogni regola di Controllo Parole Chiave vengono elencate le parole e lo stato attuale per i diversi tipi di traffico.

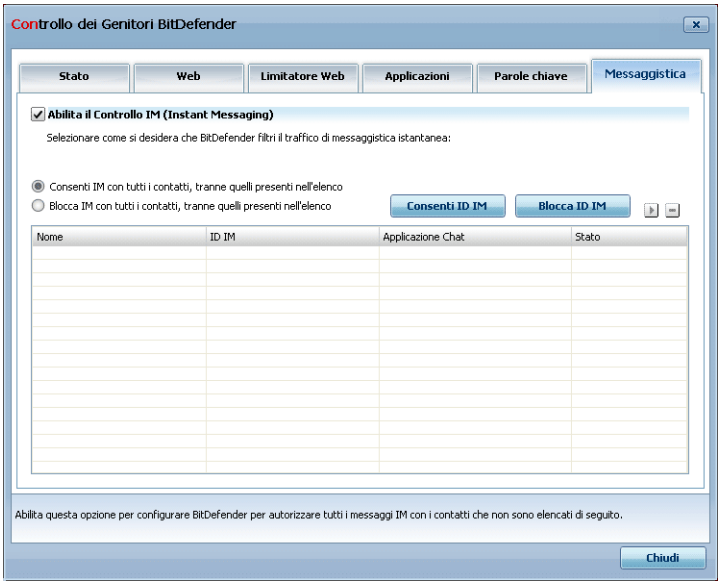
Per modificare una regola, selezionarla e fare clic sul pulsante **Modifica** e quindi eseguire le modifiche necessarie nella finestra di configurazione. Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina**.

20.7. Controllo del Chat (IM)

Il Controllo del Chat vi permette di specificare i contatti chat con i quali ai vostri bambini è permesso chattare.

Nota
Il Controllo Chat si trova disponibile solo per Yahoo Messenger and Windows Live (MSN) Messenger.

Per configurare il Controllo IM per uno specifico account utente fare clic sul pulsante **Modifica** corrispondente a tale account utente e quindi fare clic sulla scheda **Messaggistica**.


Controllo dei Genitori BitDefender
Stato
Web
Limitatore Web
Applicazioni
Parole chiave
Messaggistica
Abilita il Controllo IM (Instant Messaging)
Selezionare come si desidera che BitDefender filtri il traffico di messaggistica istantanea:
Consenti IM con tutti i contatti, tranne quelli presenti nell'elenco
Blocca IM con tutti i contatti, tranne quelli presenti nell'elenco
Consenti ID IM
Blocca ID IM
Nome
ID IM
Applicazione Chat
Stato
Abilita questa opzione per configurare BitDefender per autorizzare tutti i messaggi IM con i contatti che non sono elencati di seguito.
Chiudi

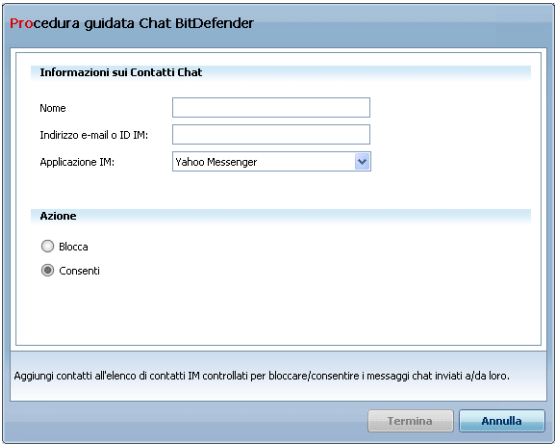
Controllo Chat

Selezionare la casella **Abilitare il Controllo del Chat** se desiderate utilizzare questa funzione di controllo.

20.7.1. Creazione di regole di controllo della messaggistica istantanea (IM)

Per permettere o bloccare la messaggistica istantanea con un contatto, seguire questi passi:

1. Fare clic su **Blocca ID IM** oppure **Permetti ID IM**. Apparirà una nuova finestra:



Aggiungi contatto Chat

2. Digitare il nome del contatto nel campo **Nome**.
3. Digitare l'indirizzo e-mail o il nome utente utilizzato dal contatto IM nel campo **E-mail o ID IM**.
4. Scegliere il programma al quale è associato il contatto.
5. Selezionare l'azione per questa regola - **Blocca** oppure **Permetti**
6. Cliccare su**OK** per aggiungere la regola.

20.7.2. Gestione di regole di controllo della messaggistica istantanea (IM)

Le regole di Controllo IM configurate sono elencate in una tabella nella parte inferiore della finestra. Per ogni regola del Controllo IM sono elencati il nome, l'ID IM, l'applicazione IM e lo stato attuale.

Per modificare una regola, selezionarla e fare clic sul pulsante **Modifica** e quindi eseguire le modifiche necessarie nella finestra di configurazione. Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina**.

Si deve inoltre selezionare quale azione deve intraprendere il Controllo Genitori di BitDefender per i contatti IM per i quali non è stata creata alcuna regola. Selezionare **Blocca** o **Permetti IM con tutti i contatti, tranne quelli nell'elenco**.

21. Controllo della Privacy

BitDefender esegue il monitoraggio di dozzine di potenziali “hotspots” nel vostro sistema dove lo spyware potrebbe agire; inoltre analizza qualsiasi cambiamento avvenuto sia nel sistema che sul software. Le minacce dello spyware sono quindi bloccate in tempo reale. Il modulo è attivo e blocca Trojan o altri codici installati da hackers, nel tentativo di compromettere la vostra privacy inviando informazioni personali, quali numeri di carte di credito per esempio, dal vostro computer ad altri.

21.1. Statistiche Controllo Privacy

Per configurare il Controllo della Privacy e visualizzare informazioni riguardanti la sua attività, andare su **Controllo della Privacy>Stato** in Modalità Avanzata.

Statistiche Controllo Privacy

Potete vedere se il Controllo della Privacy è abilitato o disabilitato. Se desiderate cambiare lo stato del Controllo della Privacy, deselezionare o selezionare la casella corrispondente.

Importante
Per evitare il furto e proteggere la vostra privacy, mantenere il **Controllo della Privacy** attivo.

Il Controllo della Privacy protegge il vostro computer utilizzando questi importanti controlli di protezione:

- Controllo Identità - protegge i vostri dati riservati filtrando tutto il traffico web (HTTP), mail (SMTP), e chat in uscita secondo le regole da voi create nella sezione Identità.
- Controllo di Registro - chiede il vostro permesso ogni volta che un programma cerca di modificare una chiave di registro per essere eseguita all'avvio di Windows.
- Controllo dei Cookie - chiederà il vostro consenso ogni volta che un sito web tenterà di impostare un cookie.
- Controllo degli Script - chiederà il vostro consenso ogni volta che un sito web tenterà di attivare uno script o un altro contenuto attivo.

Nel lato inferiore della sezione è possibile vedere le **Statistiche Controllo della Privacy**.

21.1.1. Configurazione del Livello di Protezione

Potete scegliere il livello di protezione che meglio si adatta alle vostre necessità di sicurezza. Trascinate il pulsante sulla barra per impostare il livello di protezione appropriato.

Ci sono 3 livelli di protezione:

Livello di protezione	Descrizione
Permissiva	Tutti i controlli di protezione sono disabilitati.
Default	Solo il **Controllo di Identità** è abilitato.
Aggressiva	**Controllo Identità**, **Controllo Registro**, **Controllo Cookie** e **Controllo Script** sono abilitati.

E' possibile personalizzare il livello di protezione cliccando **Livello Personalizzato**. Nella finestra che apparirà, selezionare i controlli di protezione che volete abilitare e cliccare su **OK**.

Cliccando su **Predefinito** verranno applicate le impostazioni di default.

21.2. Controllo Identità

Tenere sicuri i dati riservati è una questione importante che ci preoccupa tutti. I furto di dati ha tenuto il passo con lo siluppo delle comunicazioni via Internet e fa

uso di nuovi metodi per ingannare le persone inducendole a dare via informazioni private.

Che sia la vostra e-mail o il numero della vostra carta di credito, quando finiscono nelle mani sbagliate tali informazioni possono recarvi danno: potete trovarvi affogati nei messaggi di spam o potreste essere sorpresi nell'accedere ad un conto svuotato.

Il Controllo Identità vi protegge dal furto di dati sensibili quando siete online. Basandosi sulle regole create da voi, il Controllo Identità esegue la scansione del traffico web, mail ed instant messaging in uscita dal vostro computer, cercando specifiche sequenze di caratteri (ad esempio, la vostra carta d'identità). Se c'è una coincidenza, la pagina web, la mail o il messaggio instantaneo vengono bloccati.

Potete creare regole per proteggere ogni informazione che considerate personale o confidenziale, dal vostro numero di telefono o il vostro inidrizzo mail alle informazioni sul vostro conto in banca. Viene fornito un supporto Multi-utente, in modo che gli utenti che accedano ad altri account di Windows possano configurare ed usare le proprie regole di protezione dell'identità. Se il proprio account Windows è un account amministratore, le regole create possono essere configurate per essere applicate anche quando altri utenti del computer accedono ai rispettivi account utente Windows.

Perché usare il Controllo Identità?

- Il controllo identità è molto efficace nel bloccare lo spyware keylogger. Questo tipo di applicazione maligna registra le vostre battute sulla tastiera e le invia tramite Internet ad un hacker. L'hacker può trovare informazioni sensibili nei dati rubati, come i numeri e password di un conto corrente, ed usarle per ottenere benefici personali.

  Supponendo che tale applicazione riesca ad evitare la rilevazione antivirus, non potrà inviare i dati rubati via e-mail, web o chat se avete creato regole appropriate per la protezione dell'identità.

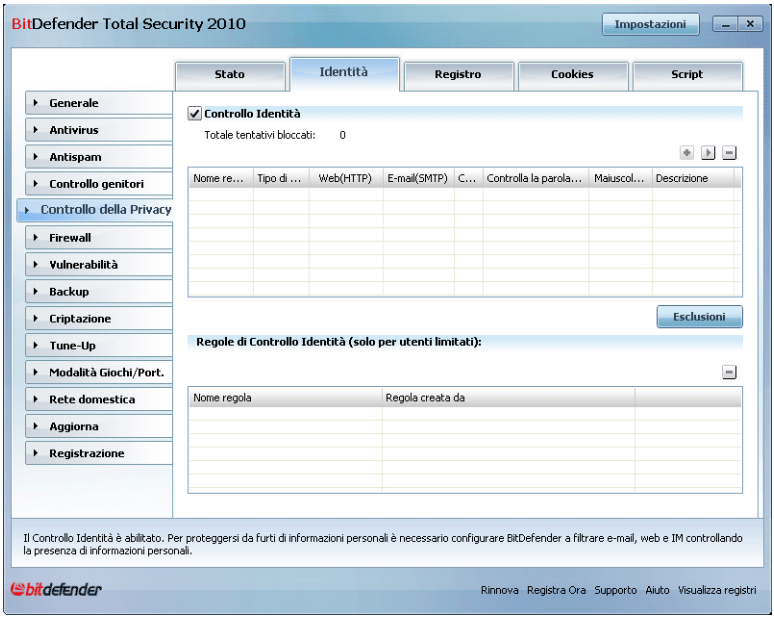
- Il Controllo identità vi può proteggere dai tentativi di phishing (tentativi di rubare informazioni personali). I tentativi più comuni di phishing fanno uso di e-mail ingannevoli per convincervi ad inviare informazioni personali ad una falsa pagina web.

  Ad esempio, potreste ricevere una mail che si proclama venire dalla vostra banca e vi richiede di aggiornare urgentemente le informazioni sul vostro conto. La mail vi fornisce un link alla pagina web dove dovreste inserire vostre informazioni personali. Anche se sembrano legittime, le mail e le pagine web alle quali vi conduce il falso link sono fasulle. Se cliccate sul link nella mail ed inviate le vostre informazioni personali alla falsa pagina web, svelerete queste informazioni alle persone che hanno organizzato il tentativo di phishing.

  Se ci sono le appropriate regole di protezione dell'identità, non potrete inviare informazioni personali (come il numero della vostra carta di credito) ad una pagina

web, a meno che non abbiate esplicitamente definito un'eccezione per questa pagina.

Per configurare il Controllo Identità, fare clic su **Controllo della Privacy>Identità** in Modalità avanzata.



Controllo Identità

Se volete usare il Controllo Identità, seguire questi passi:

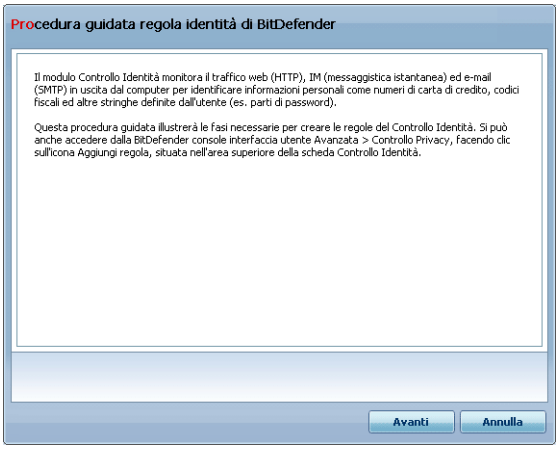
1. Selezionare la casella di controllo **Abilita controllo Identità**.
2. Creare regole per proteggere i vostri dati sensibili. Per ulteriori informazioni, vi preghiamo di riferirvi a «*Creazione delle Regole d'Identità*» (p. 247).
3. Se necessario, definire esclusioni specifiche alle regole create. Per ulteriori informazioni, vi preghiamo di riferirvi a «*Definizione Esclusioni*» (p. 250).
4. Se si è un amministratore del computer, è possibile escludere se stessi dalle regole di identità create da altri amministratori.

   Per ulteriori informazioni, fare riferimento a «*Regole definite da altri amministratori*» (p. 252).

21.2.1. Creazione delle Regole d'Identità

Per creare una regola di protezione dell'identità, fare clic sul pulsante **Aggiungi** e seguire procedura guidata di configurazione.

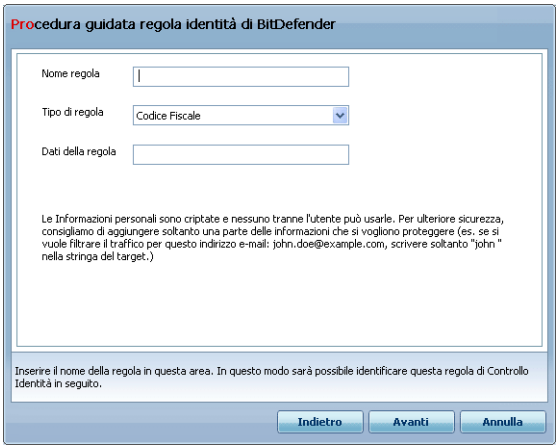
Passo 1/4 - Finestra di Benvenuto


Procedura guidata regola identità di BitDefender
Il modulo Controllo Identità monitora il traffico web (HTTP), IM (messaggistica istantanea) ed e-mail (SMTP) in uscita dal computer per identificare informazioni personali come numeri di carta di credito, codici fiscali ed altre stringhe definite dall'utente (es. parti di password).
Questa procedura guidata illustrerà le fasi necessarie per creare le regole del Controllo Identità. Si può anche accedere dalla BitDefender console interfaccia utente Avanzata > Controllo Privacy, facendo clic sull'icona Aggiungi regola, situata nell'area superiore della scheda Controllo Identità.
Avanti
Annulla

Finestra di benvenuto

Selezionare **Avanti**.

Passo 2/4 - Impostazione Tipo di Regola e Dati


Procedura guidata regola identità di BitDefender
Nome regola
Tipo di regola
Codice Fiscale
Dati della regola
Le Informazioni personali sono criptate e nessuno tranne l'utente può usarle. Per ulteriore sicurezza, consigliamo di aggiungere soltanto una parte delle informazioni che si vogliono proteggere (es. se si vuole filtrare il traffico per questo indirizzo e-mail: john.doe@example.com, scrivere soltanto "john " nella stringa del target.)
Inserire il nome della regola in questa area. In questo modo sarà possibile identificare questa regola di Controllo Identità in seguito.
Indietro
Avanti
Annulla

Impostare il Tipo di Regola e i Dati

Dovete impostare i parametri seguenti:

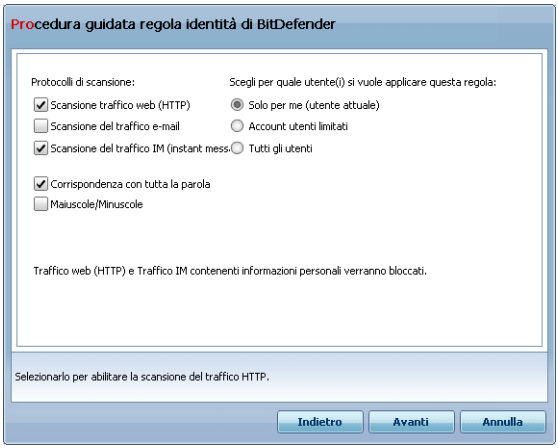
- **Nome Regola** - inserire il nome della regola nel campo di modifica.
- **Tipo di Regola** - scegliere il tipo di regola (indirizzo, nome, carta di credito, PIN, SSN etc).
- **Dati Regola** - inserire i dati da proteggere nel campo di modifica. Ad esempio, se si vuole proteggere la carta di credito, inserire tutto o parte del numero in questo campo.

> **Nota**
> Se inserite meno di tre caratteri, vi verrà chiesto di validare i dati. Vi consigliamo di inserire al meno tre caratteri per evitare il blocco erroneo di messaggi e pagine web.

Tutti i dati che inserite sono criptati. Per una sicurezza maggiore, non inserire tutti i dati che volete proteggere.

Selezionare **Avanti**.

Passo 3/4 - Selezionare i Tipi di Traffico e gli Utenti


Procedura guidata regola identità di BitDefender
Protocolli di scansione:
Scansione traffico web (HTTP)
Scansione del traffico e-mail
Scansione del traffico IM (instant mess
Corrispondenza con tutta la parola
Maiuscole/Minuscole
Scegli per quale utente(i) si vuole applicare questa regola:
Solo per me (utente attuale)
Account utenti limitati
Tutti gli utenti
Traffico web (HTTP) e Traffico IM contenenti informazioni personali verranno bloccati.
Selezionarlo per abilitare la scansione del traffico HTTP.
Indietro
Avanti
Annulla

Selezionare i Tipi di Traffico e gli Utenti

Selezionare il traffico che si desidera esaminare con BitDefender. Sono disponibili le seguenti opzioni:

- **Scansione web (traffico HTTP)** - scansiona il traffico HTTP (web) e blocca i dati in uscita corrispondenti ai dati della regola.
- **Scansione e-mail (traffico SMTP)** - esamina il traffico SMTP (mail) e blocca le mail in uscita contenenti i dati della regola.
- **Scansione IM (Instant Messaging)** - scansiona il traffico Instant Messaging e blocca i messaggi in uscita contenenti i dati della regola.

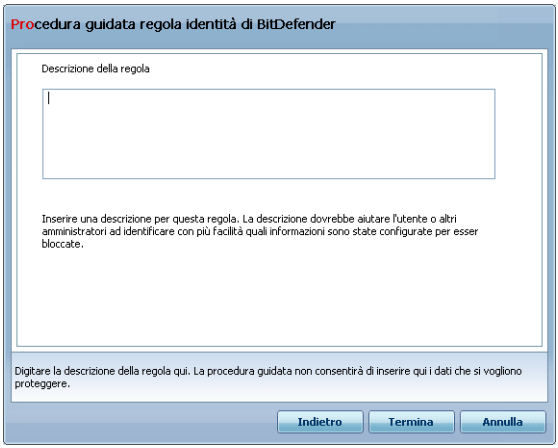
Potete scegliere di applicare la regola solo se i dati della regola corrispondono completamente oppure se le maiuscole/minuscole corrispondono.

Specificare gli utenti a cui si applica la regola.

- **Solo per me (utente attuale)** - la regola si applica solo all'account utente attuale.
- **Account utente limitati** - la regola si applica all'utente attuale e a tutti gli account di Windows limitati.
- **Tutti gli utenti** - la regola si applica a tutti gli account di Windows.

Selezionare **Avanti**.

Passo 4/4 – Descrizione Regola


Procedura guidata regola identità di BitDefender
Descrizione della regola
Inserire una descrizione per questa regola. La descrizione dovrebbe aiutare l'utente o altri amministratori ad identificare con più facilità quali informazioni sono state configurate per esser bloccate.
Digitare la descrizione della regola qui. La procedura guidata non consentirà di inserire qui i dati che si vogliono proteggere.
Indietro
Termina
Annulla

Definizione Regola

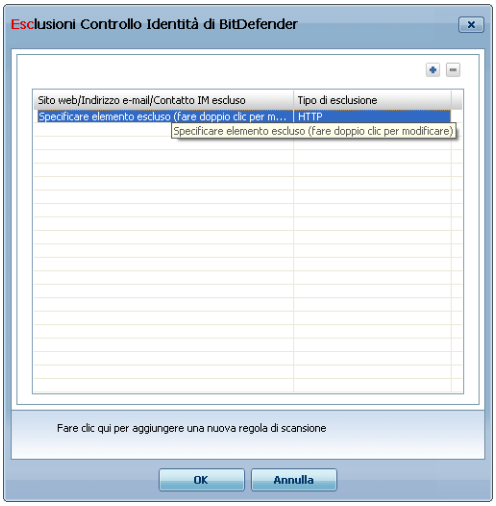
Inserire una breve descrizione della regola nel campo di editing. Siccome i dati bloccati (serie di caratteri) non vengono mostrati in plain text quando si accede alla regola, la descrizione dovrebbe aiutarvi ad identificarla facilmente.

Selezionare **Termina**. La regola apparirà nella tabella.

21.2.2. Definizione Esclusioni

Ci sono dei casi in cui dovrete definire eccezioni a specifiche regole d'identità. Consideriamo il caso in cui voi create una regola che impedisca l'invio attraverso HTTP (web) del numero della vostra carta di credito. Ogni volta che il numero della vostra carta di credito verrà inviato ad un sito web dal vostro account, la rispettiva pagina verrà bloccata. Se volete, per esempio, comprare delle scarpe in un negozio on line (che sapete che è sicuro), dovrete specificare un'eccezione alla rispettiva regola.

Per aprire la finestra dove si possono gestire le eccezioni, fare clic su **Esclusioni**.


Esclusioni Controllo Identità di BitDefender
Sito web/Indirizzo e-mail/Contatto IM escluso
Tipo di esclusione
Specificare elemento escluso (Fare doppio clic per m...
HTTP
Specificare elemento escluso (Fare doppio clic per modificare)
Fare clic qui per aggiungere una nuova regola di scansione
OK
Annulla

Esclusioni

Per aggiungere un'eccezione, seguire i seguenti passi:

1. Selezionare **Aggiungi** per aggiungere una nuova regola alla tabella.
2. Fare doppio clic su **Specifica elementi esclusi** e fornire gli indirizzi web, mail o chat che si desidera vengano aggiunti come eccezione.
3. Fare clic due volte su **Tipo traffico** e scegliere dal menu l'opzione corrispondente al tipo d'indirizzo fornito in precedenza.
   - Se avete scelto un indirizzo web, selezionare **HTTP**.
   - Se avete specificato un indirizzo mail, selezionare **E-mail (SMTP)**.
   - Se avete specificato un contatto chat, selezionare **Chat**.

Per rimuovere un'eccezione dall'elenco, selezionarla e fare clic sul pulsante **Rimuovi**.

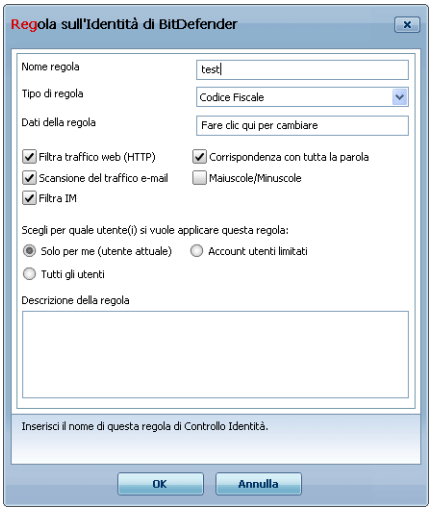
Selezionare **Applica** per salvare le modifiche.

21.2.3. Amministrazione delle regole

Potete visualizzare l'elenco delle regole create finora nella tabella.

Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina**.

Per modificare una regola, selezionarla e fare clic sul pulsante **Modifica** oppure fare doppio clic su di essa. Apparirà una nuova finestra.



Modifica Regola

Qui potete modificare il nome, la definizione e i parametri della regola (tipo, dati e traffico). Cliccate su **OK** per salvare le modifiche.

21.2.4. Regole definite da altri amministratori

Se non si è l'unico utente con diritti di amministratore sul sistema, gli altri amministratori possono creare regole di identità a proprio piacimento. Nel caso si desideri che le regole create da altri utenti non si applichino quando si è effettuato l'accesso, BitDefender permette di escludere se stessi da qualsiasi regola che non si sia creata.

È possibile vedere un elenco di regole create da altri amministratori nella tabella sotto la voce **Regole di controllo Identità**. Per ogni regola viene elencato il nome e l'utente che l'ha creata.

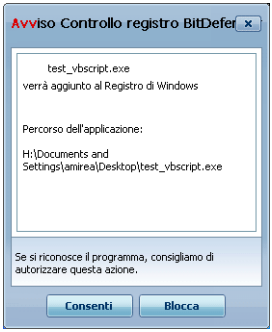
Per escludersi da una regola, selezionarla nella tabella e fare clic sul pulsante **Elimina**.

21.3. Controllo dei Registri

Una componente molto importante del sistema operativo di Windows si chiama **Registro**. E' dove Windows tiene le informazioni relative alle proprio configurazioni, ai programmi installati, all'utente e così via.

Il **Registro** è inoltre utilizzato per definire quali Programmi devono essere eseguiti automaticamente all'avvio di Windows. Spesso i virus lo utilizzano per essere eseguiti automaticamente quando l'utente riavvia il proprio computer.

Il **Controllo dei Registri** sorveglia il Registro di Windows – azione utile per rilevare i Trojan (Cavalli di Troia). Vi avviserà ogni volta che un programma tenterà di modificare una entrata del registro per poter essere eseguito all'avvio di Windows.



Allarme sul Registro

Potete vedere il programma che sta tentando di modificare il Registro di Windows.

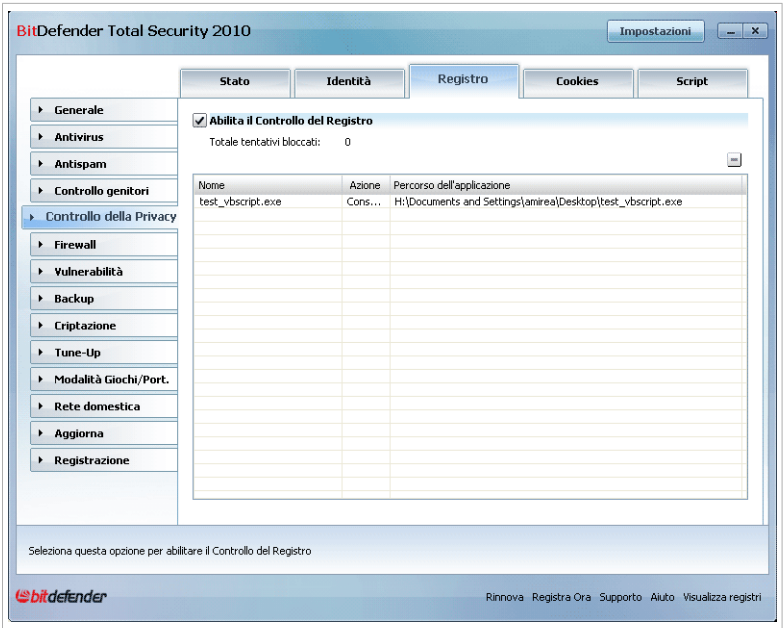
Se non riconoscete il programma e vi sembra sospetto, cliccare su **Bloccare** per impedirgli di modificare il Registro di Windows. Altrimenti, cliccare su **Consentire** per permettere la modifica.

In base alla vostra risposta, viene creata una regola e viene elencata nella tabella delle regole. La stessa azione viene applicata ogni volta che questo programma tenta di modificare una chiave di registro.

Nota

BitDefender vi avviserà, di norma, quando installerete nuovi programmi che necessitano di esecuzione immediata dopo il successivo avvio del vostro computer. Nella maggior parte dei casi questi programmi sono leciti e ci si può fidare.

Per configurare il Controllo di Registro, andare a **Controllo della Privacy>Registro** in Modalità Avanzata.



Controllo dei Registri

Potete visualizzare l'elenco delle regole create finora nella tabella.

Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina**.

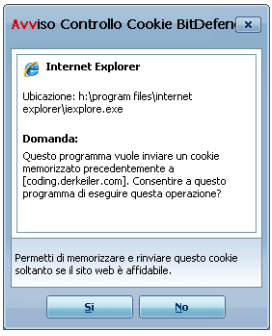
21.4. Controllo dei Cookie

I cookie sono molti frequenti su Internet. Si tratta di piccoli file immagazzinati sul vostro computer. I siti web creano questi cookie per tenere traccia di specifiche informazioni che vi riguardano.

Generalmente i Cookie vengono creati per rendere facilitare le cose. Ad esempio possono aiutare i siti web a ricordare il vostro nome e le vostre preferenze, così da non doverli inserire ad ogni visita.

I cookie però possono anche essere utilizzati per compromettere la vostra riservatezza, tenendo traccia delle vostre abitudini di navigazione.

E' qui che il **Controllo dei Cookie** vi sarà di aiuto. Quando è attivato, il **Controllo dei Cookie** chiederà il vostro permesso ogni volta che un sito web tenta di impostare un cookie:


Avviso Controllo Cookie BitDefen
Internet Explorer
Ubicazione: h:\program files\internet explorer\iexplore.exe
Domanda:
Questo programma vuole inviare un cookie memorizzato precedentemente a [coding.derkeiler.com]. Consentire a questo programma di eseguire questa operazione?
Permetti di memorizzare e rinviare questo cookie soltanto se il sito web è affidabile.
Sì
No

Allarme cookie

E' possibile visualizzare il nome dell'applicazione che sta tentando di inviare il file cookie.

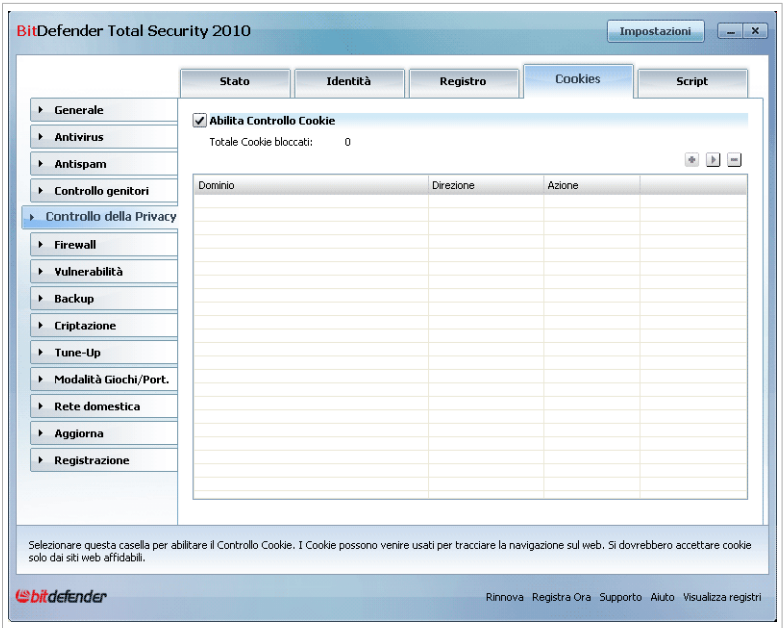
Fare clic su **Sì** o **No** e una regola verrà creata, applicata ed elencata nella tabella delle regole.

Ciò aiuterà a scegliere i siti web di cui ci si fida e quelli di cui non ci si fida.

Nota

A causa del notevole numero di cookie utilizzati oggi giorno su Internet, il **Controllo dei Cookie** può risultare inizialmente abbastanza noioso. All'inizio porrà molte domande riguardo ai siti che tentano di piazzare i cookie sul vostro computer. Non appena si aggiungeranno i vostri siti abituali all'elenco delle regole, la navigazione diventerà semplice come prima.

Per configurare il Controllo dei Cookie, fare clic su **Controllo della Privacy>Cookie** in Modalità Avanzata.



Controllo dei Cookie

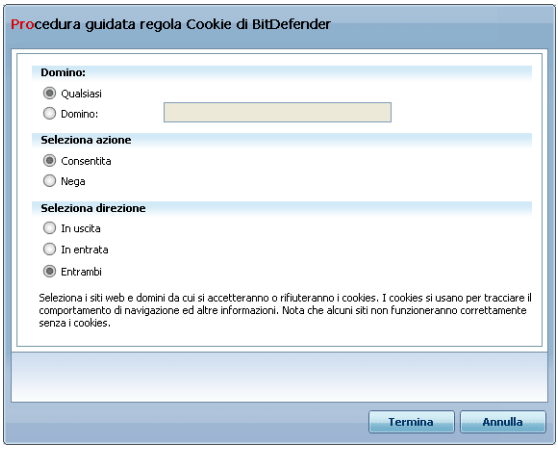
Potete visualizzare l'elenco delle regole create finora nella tabella.

Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina**. Per modificare i parametri della regola, fare clic sul pulsante **Modifica** o fare doppio clic su di essa. Eseguire i cambiamenti desiderati nella finestra di configurazione.

Per aggiungere manualmente una regola, fare clic sul pulsante **Aggiungi** e configurare i parametri della regola nella finestra di configurazione.

21.4.1. Finestra di Configurazione

Quando modificate o aggiungete manualmente una regola apparirà la finestra di configurazione.


Procedura guidata regola Cookie di BitDefender
Domino:
Qualsiasi
Domino:
Seleziona azione
Consentita
Nega
Seleziona direzione
In uscita
In entrata
Entrambi
Seleziona i siti web e domini da cui si accetteranno o rifiuteranno i cookies. I cookies si usano per tracciare il comportamento di navigazione ed altre informazioni. Nota che alcuni siti non funzioneranno correttamente senza i cookies.
Termina
Annulla

Seleziona Indirizzo, Azione e Direzione

Potete impostare i parametri:

- **Dominio** - digitare il dominio sul quale applicare la regola.
- **Azione** - selezionare l'azione della regola.

Azione	Descrizione
Permetti	I cookie da quel dominio verranno eseguiti.
Impedisci	I cookie da quel dominio non verranno eseguiti.

- **Direzione** - seleziona la direzione del traffico.

Direzione	Descrizione
In Uscita	La regola verrà applicata solo per i cookie che vengono rispediti al sito connesso.
In Entrata	La regola verrà applicata solo per i cookie che vengono ricevuti dal sito connesso.
Entrambe	La regola sarà applicata in entrambe le direzioni.

Nota
Si possono accettare i cookie, ma non conviene mai rispedirli, cioè impostando l'azioneo **Divieto** e la direzione **Uscente**.

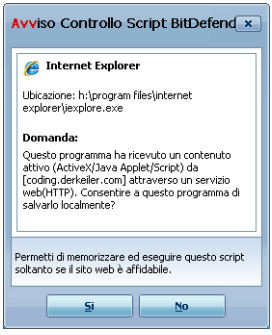
Selezionare **Termina**.

21.5. Controllo script

Gli Scripts e altri codici come ActiveX controls e Java applets, che sono utilizzati per creare pagine interattive, possono essere programmati per avere effetti dannosi. Per esempio gli elementi ActiveX , possono ottenere l' accesso ai dati del vostro computer, cancellare informazioni, catturare passwords e intercettare messaggi mentre siete online. Dovreste accettare contenuti attivi esclusivamente da siti che si conoscono come affidabili.

BitDefender vi consente di scegliere se eseguire questi elementi o bloccare la loro esecuzione.

Con il **Controllo degli Script** sarete coinvolti nel decidere di quali siti web vi fidate e di quali non vi fidate. BitDefender chiederà il vostro permesso ogni volta che un sito web tenta di attivare uno script o altri contenuti attivi:

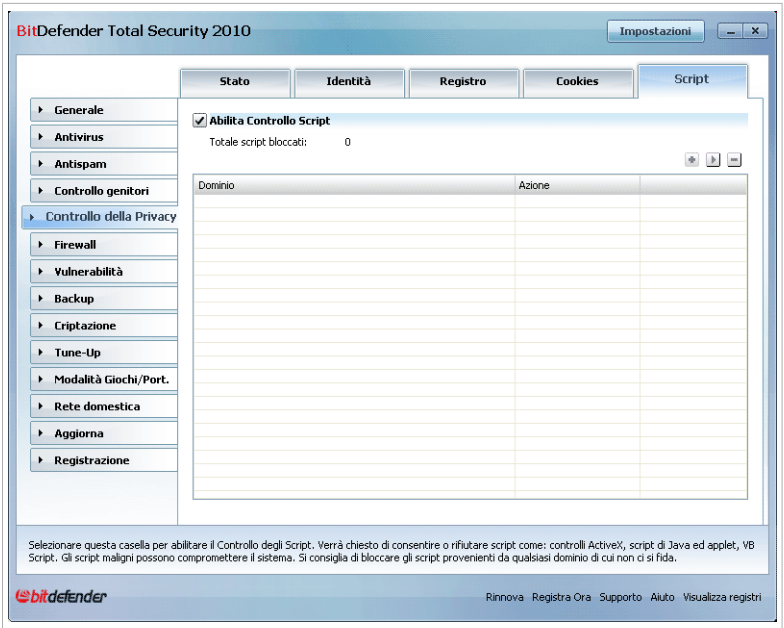

Avviso Controllo Script BitDefend
Internet Explorer
Ubicazione: h:\program files\internet explorer\iexplore.exe
Domanda:
Questo programma ha ricevuto un contenuto attivo (ActiveX/Java Applet/Script) da [coding.derkeiler.com] attraverso un servizio web(HTTP). Consentire a questo programma di salvarlo localmente?
Permetti di memorizzare ed eseguire questo script soltanto se il sito web è affidabile.
Sì
No

Allarme script

E' possibile visualizzare il nome della risorsa.

Fare clic su **Sì** o **No** e una regola verrà creata, applicata ed elencata nella tabella delle regole.

Per configurare il Controllo degli Script, fare clic su **Controllo della Privacy>Script** in Modalità Avanzata.



Controllo script

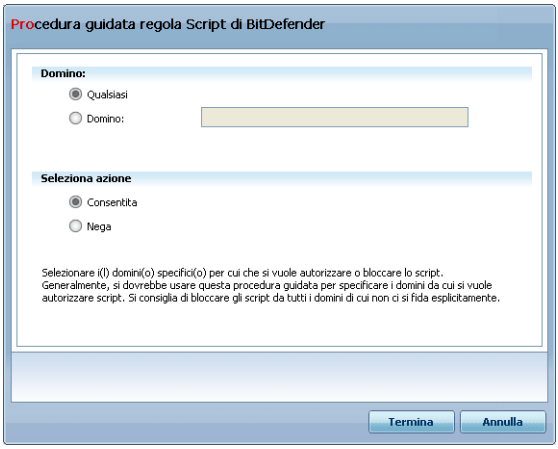
Potete visualizzare l'elenco delle regole create finora nella tabella.

Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina**. Per modificare i parametri della regola, fare clic sul pulsante **Modifica** o fare doppio clic su di essa. Eseguire i cambiamenti desiderati nella finestra di configurazione.

Per creare manualmente una regola, fare clic sul pulsante **Aggiungi** e configurare i parametri della regola nella finestra di configurazione.

21.5.1. Finestra di Configurazione

Quando modificate o aggiungete manualmente una regola apparirà la finestra di configurazione.


Procedura guidata regola Script di BitDefender
Domino:
Qualsiasi
Domino:
Seleziona azione
Consentita
Nega
Selezionare i(l) domini(o) specifici(o) per cui che si vuole autorizzare o bloccare lo script.
Generalmente, si dovrebbe usare questa procedura guidata per specificare i domini da cui si vuole autorizzare script. Si consiglia di bloccare gli script da tutti i domini di cui non ci si fida esplicitamente.
Termina
Annulla

Selezionare Indirizzo ed Azione

Potete impostare i parametri:

- **Dominio** - digitare il dominio sul quale applicare la regola.
- **Azione** - selezionare l'azione della regola.

Azione	Descrizione
Permetti	Gli script da quel dominio verranno eseguiti.
Impedisci	Gli script da quel dominio non verranno eseguiti.

Selezionare **Termina**.

22. Firewall

Il Firewall protegge il vostro computer dai tentativi di connessione non autorizzati sia in entrata che in uscita. E' come una guardia al vostro cancello – manterrà sotto controllo la vostra connessione Internet e terrà traccia di coloro ai quali si concede di accedere ad Internet e di coloro ai quali non è permesso.

Nota
Un firewall è essenziale se si dispone di una banda larga o di una connessione DSL.

In Modalità Invisibile, il vostro computer risulta "nascosto" a software maligni e hacker. Il modulo Firewall è in grado di rilevare automaticamente e proteggere il computer contro i portscan (flusso di pacchetti spediti a una macchina per trovare "punti di accesso", spesso in preparazione di un attacco).

22.1. Impostazioni

Per configurare la protezione firewall, fare clic su **Firewall>Impostazioni** in Modalità Avanzata.

Impostazioni del Firewall

Potete vedere se il firewall BitDefender è abilitato o disabilitato. Se desiderate modificare lo stato del firewall, deselezionare o selezionare la casella corrispondente.

Importante
Per essere protetti contro gli attacchi via Internet, mantenere il **Firewall** abilitato.

Ci sono due categorie di informazioni:

- **Configurazione di rete Abbreviata.** Potete vedere il nome del vostro computer, il suo indirizzo IP ed il gateway di default. Se avete più di un adattatore di rete (significa che siete connessi a più di una rete), vedrete l'indirizzo IP ed il gateway configurati per ogni adattatore.
- **Statistiche.** Potete vedere diverse statistiche riguardanti le attività del firewall:
  - numero di byte inviati.
  - numero di byte ricevuti.
  - numero di scansioni di porte rilevate e bloccate da BitDefender. Le scansioni delle porte vengono usate frequentemente dagli hackers per trovare porte aperte sul vostro computer con l'intenzione di sfruttarle.
  - numero di pacchetti persi.
  - numero di porte aperte.
  - numero di connessioni in entrata attive.
  - numero di connessioni in uscita attive.

Per vedere le connessioni attive e le porte aperte, fare clic sulla scheda Attività.

Nel lato inferiore della sezione potete vedere le statistiche BitDefender a proposito del traffico in arrivo e in uscita. Il grafico mostra il volume del traffico internet degli ultimi due minuti.

Nota
Il grafico appare anche se il **Firewall** è disabilitato.

22.1.1. Impostare l'Azione di Default

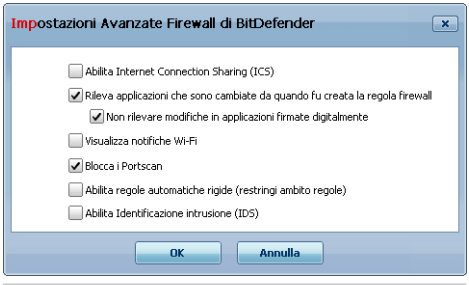
Di default, BitDefender permette automaticamente a tutti i programmi conosciuti presenti nella sua white list di accedere ai servizi di rete e ad Internet. Per tutti gli altri programmi, BitDefender vi chiede tramite una finestra di allarme di specificare l'azione da intraprendere. L'azione da voi specificata viene intrapresa ogni volta che la rispettiva applicazione richiede l'accesso alla rete / Internet.

Potete trascinare il pulsante scorrevole lungo la barra per impostare l'azione da intraprendere di default sulle applicazioni che richiedono accesso alla rete/Internet. Sono disponibili le seguenti azioni di default:

Azione di default	Descrizione
Consenti tutto	Applica le regole correnti e permette tutti i tentativi di traffico che non corrispondono con le regole correnti senza chiedere il consenso. Questa policy è vivamente sconsigliata però potrebbe essere utile per amministratori di rete e giocatori (gamers).
Consenti Programmi Conosciuti	Applica le regole correnti e consente tutti i tentativi di connessione in uscita dai programmi conosciuti come legittimi (White List) da BitDefender senza chiedere il consenso. Per il resto dei tentativi di connessione, BitDefender vi chiederà il permesso. I programmi inclusi nella White List sono le applicazioni più comunemente utilizzate al mondo. Includono i browser più conosciuti, riproduttori audio & video, programmi di chat e condivisione file, così come applicazioni client server e di sistema operativo. Per vedere la whitelist completa, fare clic su **Visualizza Whitelist**.
Report	Applica le regole correnti e chiede su tutti i tentativi di traffico che non corrispondono ad una qualunque delle regole correnti di consenso.
Rifiuta tutto	Applica le regole correnti e blocca tutti i tentativi di traffico che non corrispondono ad una qualunque delle regole correnti.

22.1.2. Configurazione delle Impostazioni Avanzate del Firewall

È possibile fare clic su **Impostazioni Avanzate** per configurare le impostazioni avanzate del firewall.


Impostazioni Avanzate Firewall di BitDefender
Abilita Internet Connection Sharing (ICS)
Rileva applicazioni che sono cambiate da quando fu creata la regola firewall
Non rilevare modifiche in applicazioni firmate digitalmente
Visualizza notifiche Wi-Fi
Blocca i Portscan
Abilita regole automatiche rigide (restringi ambito regole)
Abilita Identificazione intrusione (IDS)
OK
Annulla

Impostazioni Avanzate del Firewall

Sono disponibili le seguenti opzioni:

- **Abilita il supporto Condivisione Connessione Internet(ICS)** - abilita il supporto per la Condivisione Connessione Internet (ICS).

  Nota
  Questa opzione non abilita automaticamente ICS sul vostro sistema, ma consente solo questo tipo di connessione nel caso voi la abilitiate dal vostro sistema operativo.

  La Condivisione della Connessione Internet (ICS) permette ai membri delle reti locali di collegarsi ad Internet attraverso il vostro computer. Ciò è utile quando usufruite di una connessione Internet speciale/particolare (es. connessione wireless) e volete condividerla con altri membri della vostra rete.

  Condividere la vostra connessione Internet con i membri delle reti locali porta ad un livello di consumo risorse più alto e può comportare un certo rischio. Taglia anche alcune delle vostre porte (quelle aperte dai membri che stanno utilizzando la vostra connessione Internet).

- **Rileva applicazioni che cambiano da quando la regola di firewall è stata creata** - verifica ogni applicazione che tenta di connettersi a Internet per vedere se è stata cambiata da quando la regola che ne controlla l'accesso è stata aggiunta. Se l'applicazione è stata cambiata, verrà visualizzato un avviso per consentire o bloccare l'accesso dell'applicazione a Internet.

  Normalmente, le applicazioni vengono modificate dagli aggiornamenti. Ma c'è il rischio che vengano modificate da applicazioni malware, con il proposito di infettare il vostro computer ed altri computer in rete.

  Nota
  Vi consigliamo di mantenere attiva questa opzione e di consentire l'accesso solo alle applicazioni che vi aspettate vengano modificate dopo che la regola di controllo del loro accesso è stata creata.

  Le applicazioni segnalate si suppone che siano di fiducia e che abbiano un più alto grado di sicurezza. È possibile selezionare **Ignora le modifiche in applicazioni firmate digitalmente** per consentire alle applicazioni firmate cambiate di connettersi ad Internet senza ricevere un avviso su questo evento.

- **Visualizza notifiche wireless** - se si è connessi ad una rete wireless, mostra delle finestre informative relative a specifiche eventualità sulla rete (ad esempio, quando un nuovo computer è entrato in rete).

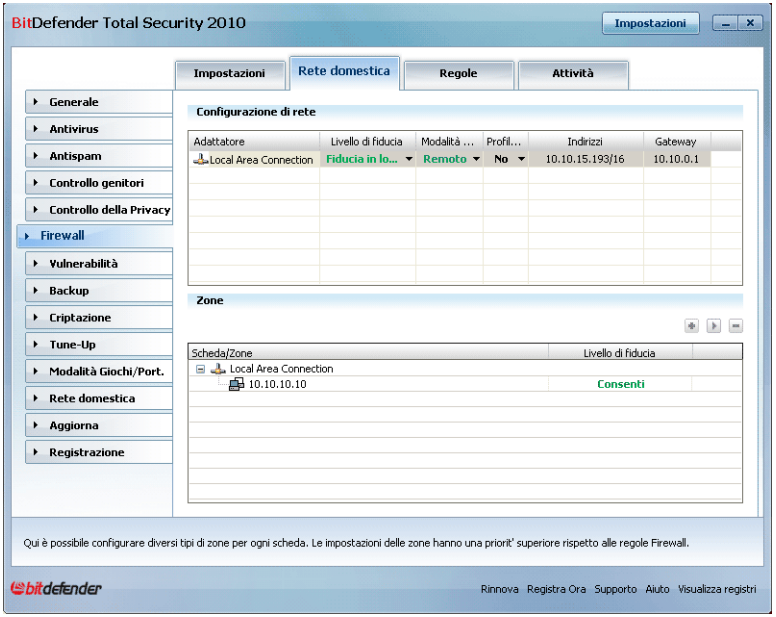
- **Bloccare le scansioni delle porte** - rileva e blocca i tentativi di scoprire quali porte sono aperte.

  Le scansioni delle porte vengono comunemente usate dai hacker per scoprire quali porte sono aperte sul vostro computer. Potrebbero quindi introdursi nel vostro computer se trovassero una porta meno sicura o vulnerabile.

- **Abilita regole automatiche rigide** - crea regole rigide utilizzando la finestra di allarme del firewall. Con questa opzione selezionata, BitDefender vi chiederà di attuare e creerà regole per ogni processo che apra l'applicazione che richieda l'accesso alla rete o ad Internet.
- **Abilita sistema di rilevamento d'intrusione (IDS)** - attiva il monitoraggio euristico delle applicazioni che tentano l'accesso ai servizi di rete o ad Internet.

22.2. Rete

Per configurare le impostazioni del firewall, fare clic su **Firewall>Rete** in Modalità Avanzata.



Rete

Le colonne della tabella **Configurazione di Rete** fornisce informazioni dettagliate sulla rete alla quale siete connessi:

- **Adattatore** - l'adattatore di rete che usa il vostro computer per connettersi alla rete o ad Internet.
- **Livello di attendibilità** - il livello di fiducia assegnato alla scheda di rete. A seconda della configurazione del adattatore di rete, BitDefender potrebbe

assegnare automaticamente all'adattatore un livello di fiducia o richiedervi ulteriori informazioni.

- **Modalità invisibile** - se si può essere rilevati da altri computer o meno.
- **Profilo generico** - se delle regole generiche vengono applicate a questa connessione o meno.
- **Indirizzi** - gli indirizzi IP configurati sull'adattatore.
- **Gateway** - l'indirizzo IP che utilizza il vostro computer per connettersi ad Internet.

22.2.1. Modifica del Livello di Fiducia

BitDefender assegna ad ogni adattatore di rete un livello di fiducia. Il livello di fiducia assegnato all'adattatore indica quanto è attendibile la corrispondente rete.

Basandosi sul livello di fiducia, delle regole specifiche vengono create per l'adattatore riguardo a come il sistema ed i processi di BitDefender accedono alla rete e ad Internet.

È possibile vedere il livello di fiducia configurato per ogni scheda nella tabella **Configurazione di Rete**, nella colonna **Livello di attendibilità**. Per modificare il livello di fiducia, fare clic sulla freccia della colonna **Livello di attendibilità** e selezionare il livello desiderato.

Livello di fiducia	Descrizione
Piena fiducia	Disabilita il firewall per il relativo adattatore.
Locale di fiducia	Consente tutto il traffico tra il vostro computer ed i computer nella rete locale.
Sicuro	Consente la condivisione di risorse con i computer nella rete locale. Questo livello viene automaticamente impostato per le reti locali (domestica o ufficio).
Non sicuro	Blocca la connessione dei computer dalla rete o da Internet al vostro computer. Questo livello viene automaticamente impostato per le reti pubbliche (se avete ricevuto un indirizzo IP da un Provider di servizi Internet)
Locale bloccato	Blocca tutto il traffico tra il vostro computer ed i computer nella rete locale mentre siete connessi ad Internet. Questo livello di fiducia viene automaticamente impostato per le reti wireless non sicure (aperte).
Bloccato	Blocca completamente la rete ed il traffico Internet attraverso il relativo adattatore.

22.2.2. Configurare la Modalità Invisibile

La Modalità Invisibile nasconde il vostro computer dal software maligno e dagli hacker in rete o in Internet. Per configurare la Modalità Invisibile, cliccare sulla freccia nella colonna **Cautela** e selezionare l'opzione desiderata.

Opzione Invisibile	Descrizione
Attivare.	La Modalità Invisibile è attiva. Il vostro computer è invisibile sia dalla rete locale che da Internet.
Disattivare	La Modalità Invisibile è disattivata Tutti possono pingare e rilevare il vostro computer dalla rete locale o da Internet.
Remoto	Il vostro computer non può essere rilevato da Internet. Gli utenti locali possono pingare e rilevare il vostro computer.

22.2.3. Configurare le Impostazioni Generali

Se l'indirizzo IP di un adattatore di rete viene modificato, BitDefender modificherà il livello di ficucia di conseguenza. Se desiderate mantenere lo stesso livello di fiducia, cliccare sulla freccia nella colonna **Generico** e selezionare **Si**.

22.2.4. Zone di rete

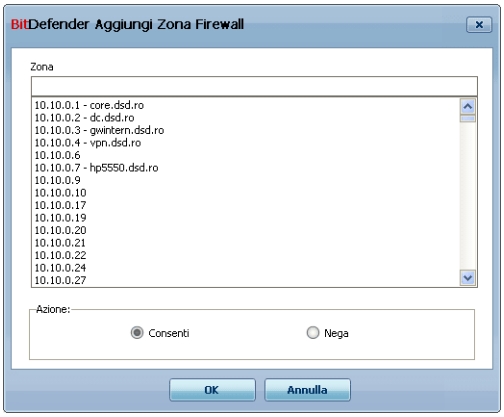
Potete aggiungere dei computer consentiti o bloccati per un adattatore specifico.

Una zona di fiducia è un computer del quale vi fidate pienamente. Tutto il traffico tra il computer ed un computer affidabile è consentito. Per condividere delle risorse con un computer specifico in una rete wireless non sicura, aggiungerli come computer consentiti.

Una zona bloccata è un computer che non volete assolutamente che comunichi con il vostro computer.

La tabella **Zone** mostra le zone di rete correnti per adattatore.

Per aggiungere una zona, fare clic sul pulsante **Aggiungi**.



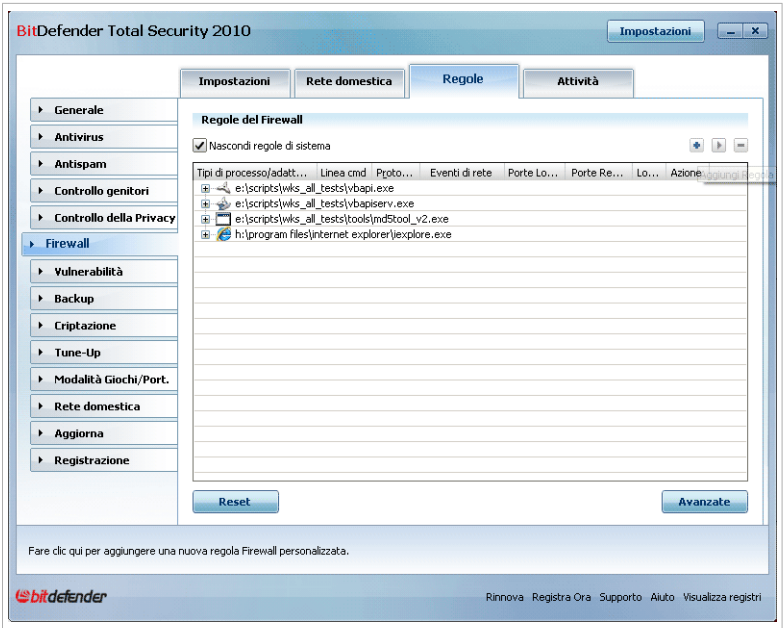
Aggiungere Zona

Procedere come segue:

1. Selezionare l'indirizzo IP del computer che volete aggiungere.
2. Selezionare l’azione:
   - **Consentire** - per consentire tutto il traffico tra il vostro computer ed il computer selezionato.
   - **Rifiutare** - per bloccare tutto il traffico tra il vostro computer ed il computer selezionato.
3. Selezionare **OK**.

22.3. Regole

Per gestire le regole del firewall che controllano l'accesso delle applicazioni alle risorse di rete o ad Internet, andare su **Firewall>Regole** in Modalità Avanzata.



Regole del Firewall

Potete vedere le applicazioni (processi) per le quali le regole del firewall sono state create. Deselezionare la casella **Nascondere le regole di sistema** se desiderate vedere anche le regole relative al sistema o ai processi di BitDefender.

Per vedere le regole create per un'applicazione specifica, cliccare sulla casella + accanto alla relativa applicazione. Potete sapere le informazioni dettagliate su ogni regola, come indicato nelle colonne della tabella:

- **Tipologie di processo/adattatore** - le tipologie di processo e adattatore di rete sui quali vengono applicate le regole. Le regole vengono create automaticamente per filtrare l'accesso alla rete o ad Internet attraverso tutti gli adattatori. Potete creare nuove regole manualmente o modificare regole esistenti per filtrare l'accesso alla rete o ad Internet di un'applicazione attraverso un adattatore specifico (ad esempio, un adattatore di rete wireless).
- **Linea di Comando** - il comando utilizzato per iniziare il processo nell'interfaccia della linea di comando di Windows (**cmd**).
- **Protocollo** - il protocollo IP al quale si applica la regola. Potrete visualizzare uno dei seguenti:

Protocollo	Descrizione
Qualsiasi	Include tutti i protocolli IP.
TCP	Transmission Control Protocol – Il Protocollo TCP abilita due host a stabilire una connessione e a scambiarsi pacchetti di dati. TCP garantisce la consegna dei dati e anche le garanzie che i pacchetti saranno consegnati nello stesso ordine in cui sono stati inviati.
UDP	User Datagram Protocol – UDP è un IP progettato per prestazioni hig. I giochi e altre applicazioni video utilizzano spesso UDP.
Un numero	Rappresenta un protocollo IP specifico (diverso da TCP e UDP). Potete trovare l'elenco completo dei numeri di protocolli IP assegnati su www.iana.org/assignments/protocol-numbers.

- **Eventi di Rete** - gli eventi di rete sui quali viene applicata la regola. I seguenti eventi possono essere tenuti in conto:

Evento	Descrizione
Connettere	Scambio preliminare di messaggi standard usati da protocolli orientati alla connessione (come il TCP) per stabilire una connessione. Con protocolli orientati alla connessione, il traffico di dati tra due computer accade solo dopo che la connessione è stabilita.
Traffico	Flusso di dati tra due computer.
Ascoltare	Stato in cui una applicazione monitorizza la rete in attesa di stabilire una connessione o di ricevere informazioni da un'applicazione pari.

- **Porte Locali** - le porte del vostro computer sulle quali la regola viene applicata.
- **Porte Remote** - le porte di computer remoti sulle quali la regola viene applicata.
- **Locale** - se la regola viene applicata solo sui computer nella rete locale.
- **Azione** - se all'applicazione è permesso o vietato l'accesso alla rete o ad Internet sotto le circostanze specificate.

22.3.1. Aggiungere Regole Automaticamente

Con il **Firewall** abilitato, BitDefender chiederà il vostro consenso ogni volta che viene eseguita una connessione ad Internet:

Allarmi del Firewall

Potete vedere quanto segue: l'applicazione che sta provando ad accedere ad Internet, il percorso per il file dell'applicazione, la destinazione, il protocollo utilizzato e la porta sulla quale l'applicazione sta provando a connettersi.

Cliccare **Consentire** per permettere tutto il traffico (in entrata ed in uscita) generato da questa applicazione dall'host locale verso qualsiasi destinazione, attraverso il rispettivo protocollo IP e su tutte le porte. Se cliccate su **Bloccare**, all'applicazione verrà completamente negato l'accesso ad Internet attraverso il rispettivo protocollo IP.

Basandosi sulla vostra risposta, una regola verrà creata, applicata ed inserita nella tabella. La prossima voltra che l'applicazione cercherà di connettersi, questa regola verrà applicata di default.

Importante
Consentire tentativi di connessioni in ingresso solo da IP o domini dei quali vi fidate.

22.3.2. Eliminazione e ripristino delle regole

Per cancellare una regola, selezionarla e cliccare sul tasto **Rimuovere regola**. Potete selezionare ed eliminare diverse regole alla volta.

Se desiderate cancellare tutte le regole create per un'applicazione specifica, selezionare l'applicazione dall'elenco e cliccare sul tasto **Rimuovere regola**.

Se si desidera caricare la regola predefinita per il livello di attendibilità selezionato, fare clic su **Ripristino regole**.

22.3.3. Creare e modificare delle Regole

Creare nuove regole manualmente e modificare regole esistenti consiste in configurare i parametri della regola nella finestra di configurazione.

Creare Regole. Per creare una regola manualmente, seguire questi passaggi:

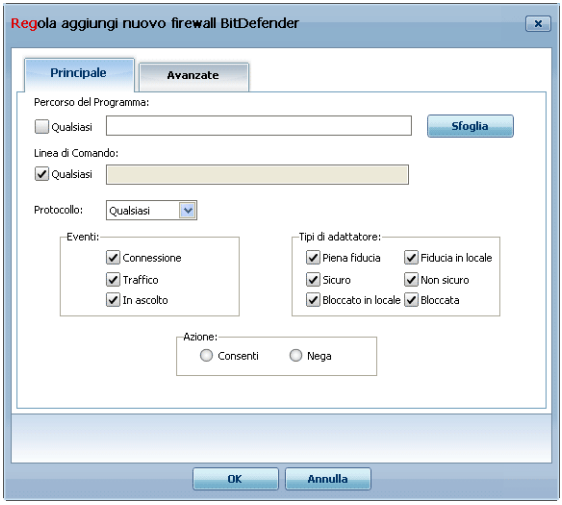
1. Fare clic sul pulsante **Aggiungi regola**. Apparirà la finestra di configurazione.
2. Configurare i parametri principali ed avanzati come necessario.
3. Cliccare su **OK** per aggiungere la nuova regola.

Modificare Regole. Per modificare una regola esistente, seguire i seguenti passaggi:

1. Fare clic sul pulsante **Modifica regola** o fare doppio clic sulla regola. Apparirà la finestra di configurazione.
2. Configurare i parametri principali ed avanzati come necessario.
3. Selezionare **Applica** per salvare le modifiche.

Configurazione dei parametri principali

La scheda **Principali** della finestra di configurazione permette di configurare i parametri principali della regola.



Parametri Principali

E' possibile configurare i seguenti parametri:

- **Percorso del Programma.** Cliccare su **Sfoglia** e selezionare l'applicazione sulla quale viene applicata la regola. Se desiderate che la regola venga applicata su tutte le applicazioni, selezionare **Qualsiasi**.
- **Linea di commando.** Se volete che la regola venga applicata solo quando l'applicazione sia aperta con un comando specifico nell'interfaccia linea di comando di Windows, deselezionare la casella **Qualsiasi** e digitare il comando corrispondente nel campo di modifica.
- **Protocollo.** Selezionare dal menu, il protocollo IP sul quale la regola verrà applicata.
  - Se desiderate che la regola venga applicata su tutti i protocolli, selezionare **Qualsiasi**.

- Se si desidera che la regola venga applicata a TCP, selezionare **TCP**.
- Se si desidera che la regola venga applicata a UDP, selezionare **UDP**.
- Se volete che la regola venga applicata su un protocollo specifico, selezionare **Altro**. Apparirà un campo di modifica. Digitare il numero assegnato al protocollo che volete filtrare nel campo di modifica.

Nota

I numeri dei protocolli IP vengono assegnati dalla Internet Assigned Numbers Authority (IANA). Potete trovare l'elenco completo dei numeri di protocolli IP assegnati su www.iana.org/assignments/protocol-numbers.

- **Eventi.** A seconda del protocollo selezionato, scegliere gli eventi di rete sui quali la regola verrà applicata. I seguenti eventi possono essere tenuti in conto:

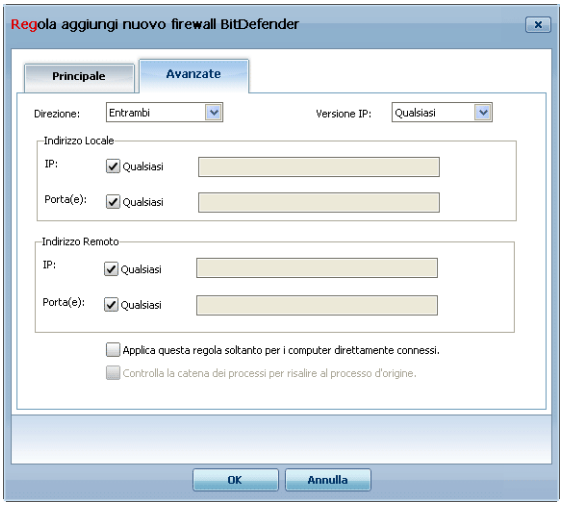
Evento	Descrizione
Connettere	Scambio preliminare di messaggi standard usati da protocolli orientati alla connessione (come il TCP) per stabilire una connessione. Con protocolli orientati alla connessione, il traffico di dati tra due computer accade solo dopo che la connessione è stabilita.
Traffico	Flusso di dati tra due computer.
Ascoltare	Stato in cui una applicazione monitorizza la rete in attesa di stabilire una connessione o di ricevere informazioni da un'applicazione pari.

- **Tipi di adattore:** Selezionare i tipi di adattatore a cui si applica la regola.
- **Azione.** Selezionare una delle azioni disponibili:

Azione	Descrizione
Permetti	L'accesso alla rete / Internet dell'applicazione verrà autorizzato quando si verifichino le circostanze specificate.
Impedisci	L'accesso alla rete / Internet dell'applicazione verrà negato le circostanze specificate.

Configurazione dei Parametri Avanzati

La scheda **Avanzati** della finestra di configurazione consente di configurare i parametri avanzati della regola.



Parametri Avanzati

Potete configurare i seguenti parametri avanzati:

- **Direzione.** Selezionare dal menu la direzione del traffico sulla quale verrà applicata la regola.

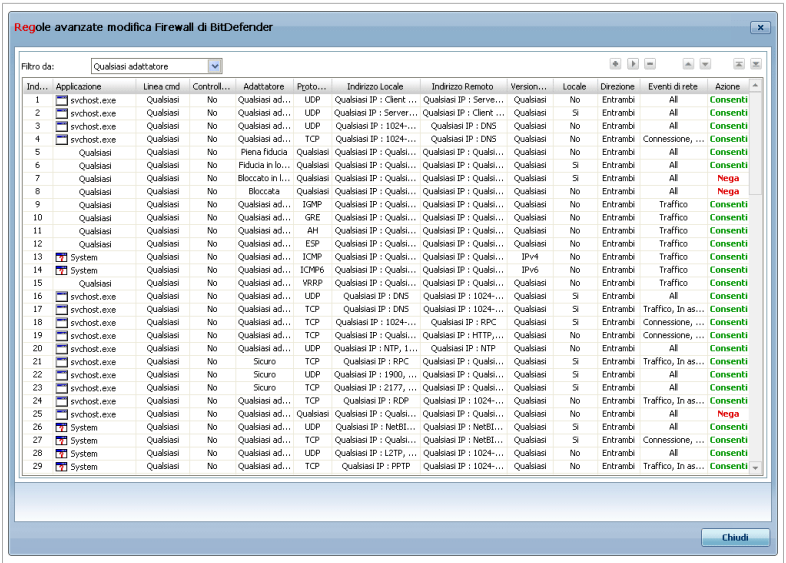
Direzione	Descrizione
In Uscita	La regola sarà applicata solo per il traffico in uscita.
In Entrata	La regola sarà applicata solo per il traffico in entrata.
Entrambe	La regola sarà applicata in entrambe le direzioni.

- **Versione IP.** Selezionare dal menu la versione IP (IPv4, IPv6 o altre) sulla quale verrà applicata la regola.
- **Indirizzo Locale.** Specificare l'indirizzo IP locale e la porta sui quali verrà applicata la regola come segue:
  - Se avete più di un adattatore di rete, potete deselezionare la casella **Qualsiasi** e digitare un indirizzo IP specifico.
  - Se avete selezionato TCP o UDP come protocollo, potete impostare una porta specifica oppure un range tra 0 e 65535. Se volete la regola applicata per tutte le porte, selezionare **Qualsiasi**.

- **Indirizzo Remoto.** Specificare l'indirizzo IP remoto e la porta sui quali verrà applicata la regola come segue:
  - Per filtrare il traffico tra il vostro computer ed un computer specifico, deselezionare la casella **Qualsiasi** e digitare il suo indirizzo IP.
  - Se avete selezionato TCP o UDP come protocollo, potete impostare una porta specifica oppure un range tra 0 e 65535. Se volete la regola applicata per tutte le porte, selezionare **Qualsiasi**.
- **Applicare questa regola solo su computer connessi direttamente.** Selezionare questa opzione quando volete che la regola venga applicata solo sui tentativi di traffico locale.
- **Controlla la catena dei processi per il processo d'origine.** È possibile modificare questo parametro solo se si seleziona **Regole automatiche rigide** (fare clic sulla scheda Impostazioni e fare clic su **Impostazioni Avanzate**). Il controllo approfondito applicazione significa che BitDefender domanda l'azione da intraprendere quando un'applicazione richiede l'accesso ad Internet/LAN da un processo parente differente (es: la richiesta di accesso ad Internet da parte di Windows Media Player all'interno di Internet Explorer)

22.3.4. Gestione Avanzata delle Regole

Se avete bisogno del controllo avanzato delle regole del firewall, cliccare su **Avanzate**. Apparirà una nuova finestra.



Gestione Avanzata delle Regole

Potete vedere le regole del firewall, elencate nell'ordine in cui sono state inserite. Le collonne della tabella forniscono informazioni esaustive su ogni regola.

Nota

Quando viene effettuato un tentativo di connessione (sia in entrata che in uscita), BitDefender applica l'azione della prima regola che corrisponde con la connessione. Per questo è molto importante l'ordine in cui le regole vengono selezionate.

Per cancellare una regola, selezionarla e fare clic sul pulsante **Elimina regola**.

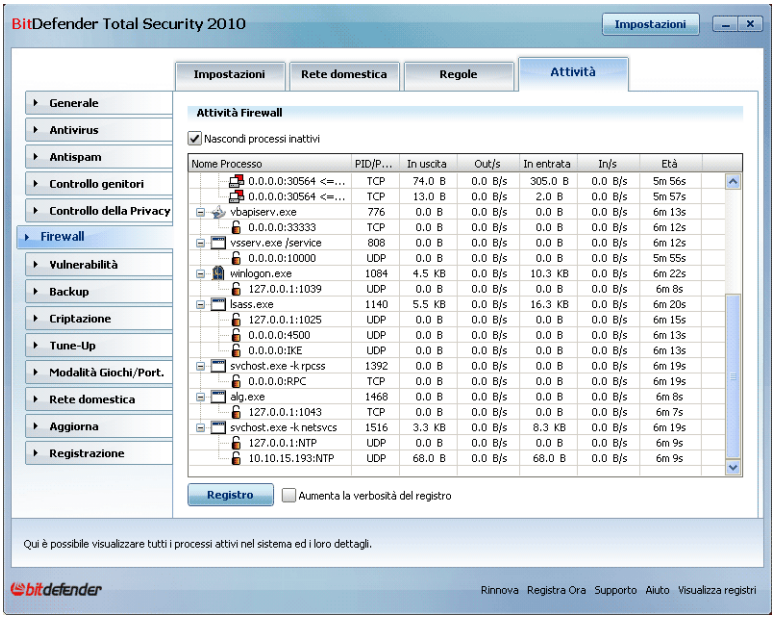
Per modificare una regola esistente, selezionarla e fare clic sul pulsante **Modifica regola** oppure fare doppio clic sulla regola.

Potete alzare o abbassare la priorità di una regola. Fare un clck sul bottone **Sposta in alto** per alzare la priorità della regola selezionata di un livello, oppure fare un click sul bottone **Sposta in basso** per abbassare la priorità della regola selezionata, di un livello. Per assegnare ad una regola la massima priorità fare clic sul pulsante **Sposta all'inizio**. Per assegnare ad una regola la minima priorità fare clic sul pulsante **Sposta alla fine**.

Cliccare su **Chiudere** per chiudere la finestra.

22.4. Controllo Connessione

Per monitorare l'attività della rete / Internet corrente (su TCP e UDP) ordinata per applicazioni ed aprire il log del Firewall BitDefender, fare clic su **Firewall>Attività** in Modalità Avanzata.



Controllo Connessione

E' possibile visualizzare il traffico totale generato dall'applicazione. Per ogni applicazione, è possibile visualizzare le connessioni e le porte aperte, così come le statistiche riguardanti la velocità del traffico in uscita ed in entrata e la quantità totale di dati inviati / ricevuti.

Se desiderate vedere anche i processi inattivi, deselezionare la casella **Nascondere processi inattivi**.

Il significato delle icone è come segue:

- Indica una connessione in uscita.
- Indica una connessione in entrata.
- Indica una porta aperta sul vostro computer.

La finestra presenta l'attività della rete corrente / Internet in tempo reale. Se le connessioni o le porte fossero chiuse, potreste vedere che le statistiche

corrispondenti sarebbero opache e che, alla fine, scomparirebbero. La stessa cosa accade a tutte le statistiche corrispondenti ad un'applicazione che genera traffico o ha delle porte aperte e che voi chiudete.

Per un elenco esauriente di eventi riguardanti l'utilizzo del modulo Firewall (abilitare/disabilitare il firewall, bloccare il traffico, modificare le impostazioni) o generati dalle attività rilevate da questo modulo (scansione delle porte, blocco di tentativi di connessione o del traffico secondo le regole), visualizzare il file di registro del Firewall BitDefender facendo clic su **Visualizza Registro**. Il file si trova nella cartella File Comuni dell'utente corrente di Windows, nel percorso: `...BitDefender\BitDefender Firewall\bdfirewall.txt`.

Se desiderate che il registro contenga più informazioni, selezionare **Incrementare verbosità del registro**.

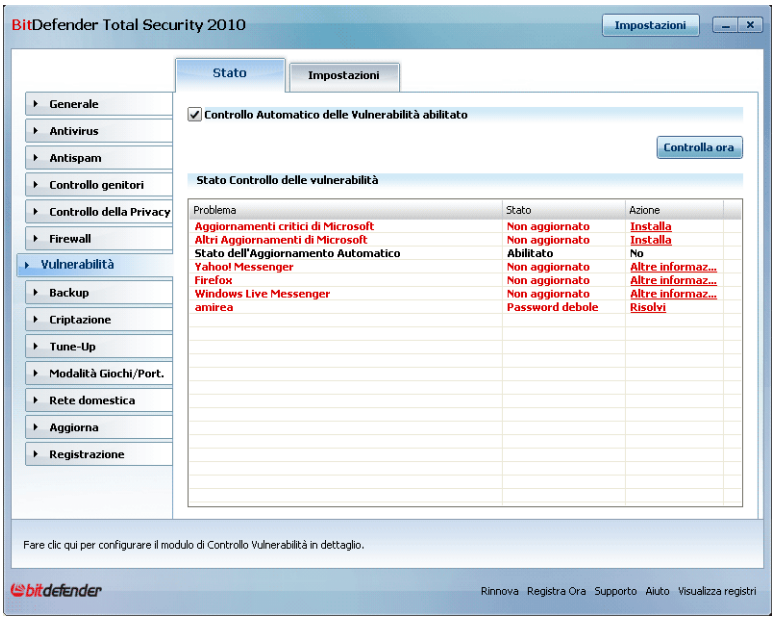
23. Vulnerabilità

Un passaggio importante nella protezione del vostro computer contro hackers e applicazioni maligne è mantenere aggiornato il sistema operativo e le applicazioni che usate regolarmente. Inoltre, per impedire accessi fisici non autorizzati al vostro computer, dovete configurare password forti (password che non possano essere facilmente indovinate) per ogni account di Windows.

BitDefender controlla regolarmente il vostro sistema alla ricerca di vulnerabilità e vi avverte dei problemi esistenti.

23.1. Stato

Per configurare il controllo automatico delle vulnerabilità o per eseguire un controllo delle vulnerabilità, fare clic su **Vulnerabilità>Stato** in Modalità Avanzata.



Stato Vulnerabilità

La tabella mostra i problemi trovati nell'ultima scansione delle vulnerabilità e il loro stato. Potete vedere l'azione intrapresa per riparare le vulnerabilità, se necessario. Se l'azione **negativa** allora il rispettivo problema non rappresenta una vulnerabilità.

Importante

Per essere avvertiti automaticamente sulle vulnerabilità del sistema o delle applicazioni, mantenere il **Controllo Automatico delle Vulnerabilità** abilitato.

23.1.1. Correggi Vulnerabilità

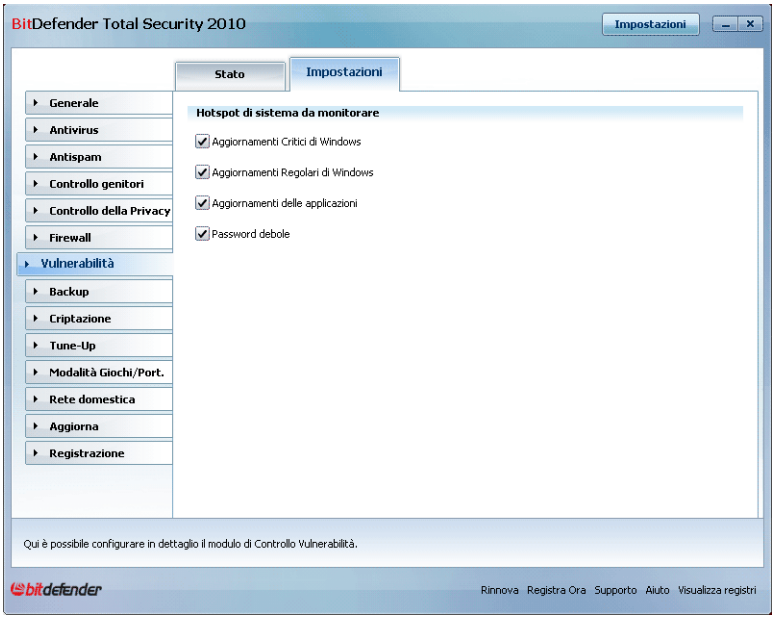
A seconda del problema, per risolvere una vulnerabilità specifica procedere come segue:

- Se sono disponibili aggiornamenti di Windows, fare clic su **Installa** nella colonna **Azione** per installarli.
- Se un'applicazione non è aggiornata, cliccare sul link fornito **Home Page** per scaricare la versione più recente.
- Se un account utente Windows ha una password debole, fare clic su **Risolvi** per costringere l'utente a modificare la password al prossimo accesso, oppure cambiate voi stessi la password. Per avere una password forte, utilizzare una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @).

Per controllare le possibili vulnerabilità del vostro computer, clicca su **Controlla adesso** e seguire la procedura guidata. Per ulteriori informazioni fare riferimento a *«Procedura guidata di Controllo delle vulnerabilità»* (p. 69).

23.2. Impostazioni

Per configurare le impostazioni del controllo automatico delle vulnerabilità andare su **Vulnerabilità>Impostazioni** in Modalità Avanzata.



Impostazioni del Controllo Automatico delle Vulnerabilità

Selezionare le caselle corrispondenti alle vulnerabilità del sistema che volete vengano controllate regolarmente.

- **Aggiornamenti Critici di Windows**
- **Aggiornamenti Regolari di Windows**
- **Aggiornamenti applicazioni**
- **Password Deboli**

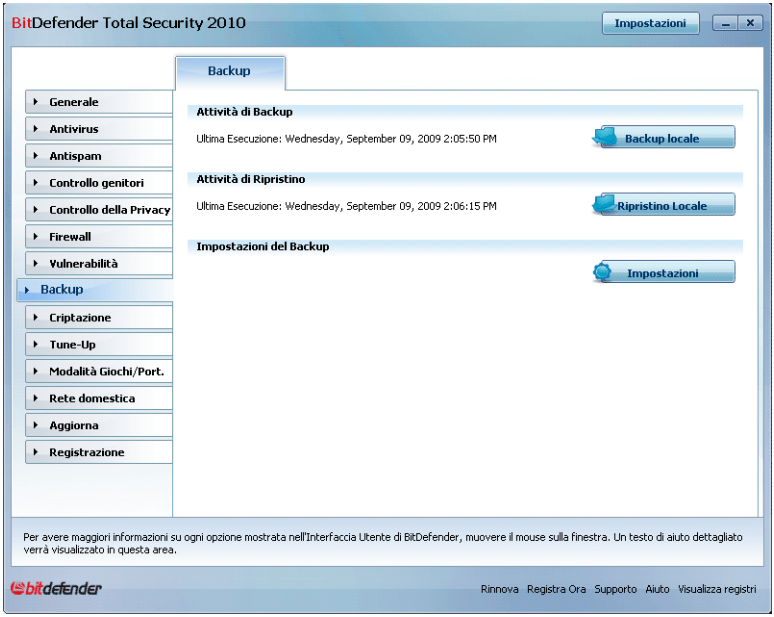
Nota

Se deselezionate la casella corrispondente ad una vulnerabilità specifica, BitDefender non vi avvertirà più sui relativi problemi.

24. Backup

BitDefender arriva con un modulo di backup che vi aiuta a fare copie di riserva di ogni prezioso dato sul vostro sistema. Potete eseguire il backup dei dati sul vostro computer, su dischi rimuovibili o su di una ubicazione di rete per essere sicuri di poter ripristinarli quando sia necessario. Il ripristino dei vostri dati è un processo facile.

Per effettuare un backup dei dati, andare su **Backup** in Modalità Avanzata.



Attività di Backup

Sono disponibili i seguenti tasti:

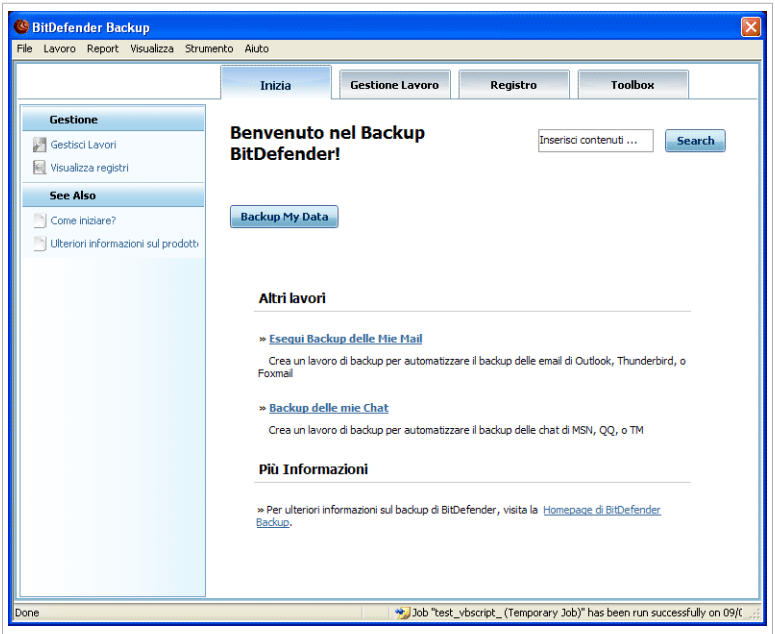
- **Backup locale** - inizia una facile procedura di cinque passi per eseguire il backup dei dati localmente.
- **Ripristino Locale** - avvia una facile procedura di quattro passaggi per eseguire il ripristino dei vostri dati localmente.
- **Impostazioni** - apre Backup BitDefender, che permette di impostare ed eseguire operazioni di backup in dettaglio.

24.1. Impostazioni del Backup

Se avete bisogno di eseguire delle operazioni di backup e ripristino più complesse, potete utilizzare la soluzione di Backup di BitDefender con delle funzionalità più complete. Backup BitDefender offre:

- una varietà di opzioni di backup, come compressione, criptazione, filtraggio dei file o impostazione della velocità di backup.
- controllo raffinato durante il ripristino dei file (ad esempio, potete ripristinare i dati sui quali avete eseguito il backup in un momento specifico).
- capacità avanzate di programmazione (ad esempio, potete scegliere di iniziare il lavoro di backup all'avvio del sistema o quando il computer si trovi inattivo)
- un visualizzatore dei log che vi aiuta a tenere traccia delle operazioni di backup e ripristino che eseguite e la risoluzione di eventuali errori.

Per aprire BitDefenser Backup, fare clic su **Impostazioni**.


BitDefender Backup
File Lavoro Report Visualizza Strumento Aiuto
Inizia
Gestione Lavoro
Registro
Toolbox
Gestione
Gestisci Lavori
Visualizza registri
See Also
Come iniziare?
Ulteriori informazioni sul prodotto
Benvenuto nel Backup BitDefender!
Inserisci contenuti ...
Search
Backup My Data
Altri lavori
» Esegui Backup delle Mie Mail
Crea un lavoro di backup per automatizzare il backup delle email di Outlook, Thunderbird, o Foxmail
» Backup delle mie Chat
Crea un lavoro di backup per automatizzare il backup delle chat di MSN, QQ, o TM
Più Informazioni
» Per ulteriori informazioni sul backup di BitDefender, visita la Homepage di BitDefender Backup.
Done
Job "test_vbscript_(Temporary Job)" has been run successfully on 09/(

BitDefender Backup

Ci sono due modi in cui si possono impostare ed eseguire le operazioni di backup. Potete utilizzare la **Barra di Menu** nella parte superiore, o cliccare una certa sezione della **Barra di Navigazione**.

La **Barra di Navigazione**, situata in alto nella finestra principale e sotto la **Barra di Menu**, da accesso a quattro sezioni:

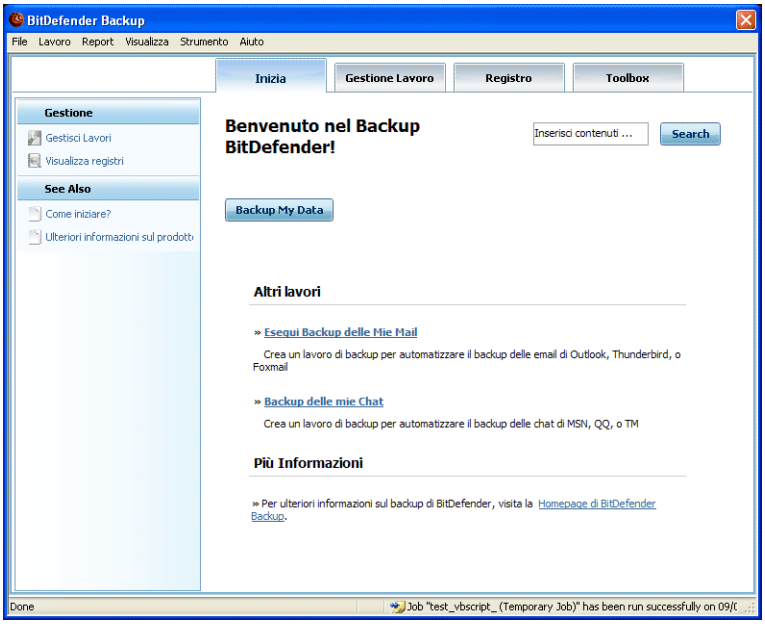
- **Iniziare**
- **Gestione Lavori**
- **Visualizzatore di Registro**
- **Toolbox**

24.1.1. Inizia

Iniziare vi aiuta ad eseguire facilmente il backup delle vostre mail, chat e dati.

Potete procedere ad **Iniziare** faccendo come segue:

- Cliccare su **Iniziare** nella **Barra di Navigazione**.
- Cliccare su **Visualizzare** nella **Barrra di Menu** e selezionare **Iniziare**.
- Utilizzare il collegamento premendo **CTRL+Alt+S**.


BitDefender Backup
File Lavoro Report Visualizza Strumento Aiuto
Inizia
Gestione Lavoro
Registro
Toolbox
Gestione
Gestisci Lavori
Visualizza registri
See Also
Come iniziare?
Ulteriori informazioni sul prodotto
Benvenuto nel Backup BitDefender!
Inserisci contenuti ...
Search
Backup My Data
Altri lavori
» Esegui Backup delle Mie Mail
Crea un lavoro di backup per automatizzare il backup delle email di Outlook, Thunderbird, o Foxmail
» Backup delle mie Chat
Crea un lavoro di backup per automatizzare il backup delle chat di MSN, QQ, o TM
Più Informazioni
» Per ulteriori informazioni sul backup di BitDefender, visita la Homepage di BitDefender Backup.
Done
Job "test_vbscript_ (Temporary Job)" has been run successfully on 09/(

Inizia

Per eseguire il backup dei documenti chiave, foto, e-mail e registri di chat durante lo stesso processo, fare clic sul tasto **Esegui il Backup dei Miei Dati** e eseguire la procedura che consiste di tre passi.

Per eseguire il backup solo delle e-mail, fare clic sul pulsante **Esegui il Backup delle Mie E-Mail** ed eseguire la procedura che consiste di tre passi.

Per eseguire il backup solo dei registri di chat, fare clic sul pulsante **Esegui il Backup dei Miei Registri di Chat** ed eseguire la procedura che consiste di tre passi.

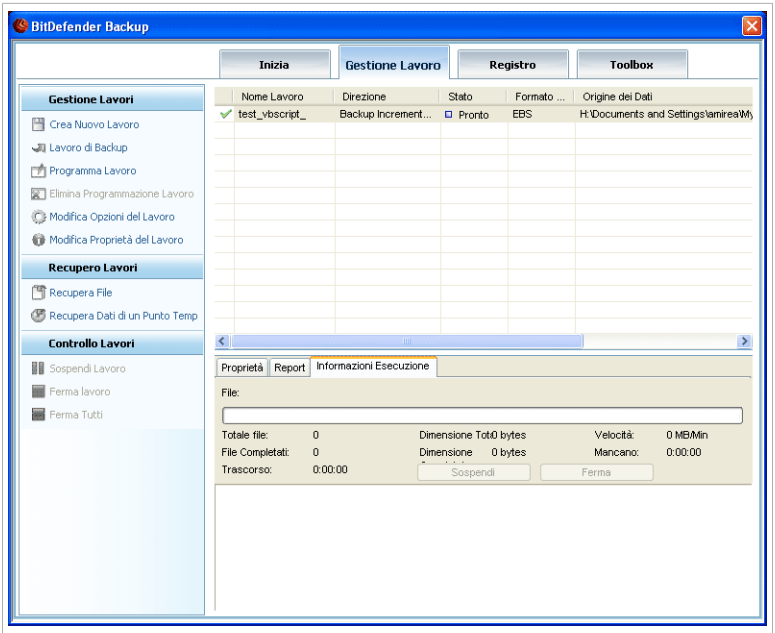
Nota
La procedura in tre fasi è descritta alla sezione *«Crea nuovo processo»* (p. 287).

24.1.2. Gestione processo

La **Gestione Lavori** viene utilizzata per visualizzare e gestire i lavori di backup, visualizzare le proprietà ed i report dei lavori, così come per monitorare la velocità di esecuzione. **Gestione Lavori** permette anche di controllare le proprietà del lavoro e lo stato corrente, di modificare le sue impostazioni, così come di eseguire il backup o il ripristino di esso.

Potete passare a **Gestione Lavori** faccendo come segue:

- Cliccare su **Gestiore Lavori** nella **Barra di Navigazione**.
- Cliccare su **Visualizzare** nella **Barra di Menu** e selezionare **Gestione Lavori**.
- Utilizzare un collegamento, premendo **CTRL+Alt+M**.



Gestione processo

Sulla sinistra, vedrete un elenco di links per operazioni veloci come segue:

Gestione Lavori

- **Creare Nuovo Lavoro**
- **Lavoro di Backup**
- **Lavoro programmato**
- **Eliminare Programmazione Lavoro**
- **Modificare Opzioni del Lavoro**
- **Modificare Proprietà del Lavoro**

Recupero Lavoro

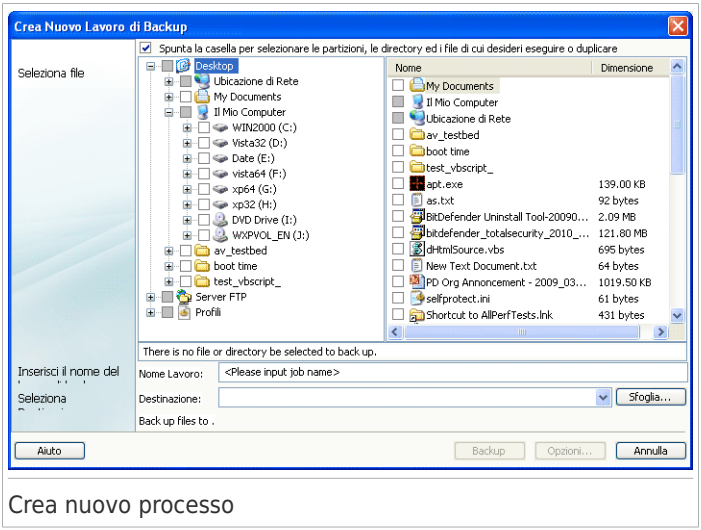
- **Ripristinare File**
- **Ripristinare Dati di un punto temporale**

Controllo Lavoro

- **Sospendere Lavoro**
- **Fermare Lavoro**
- **Fermare tutti**

Crea nuovo processo

Per eseguire il backup dei documenti chiave, foto, e-mail e registri di chat durante lo stesso processo, fare clic sul pulsante **Crea Nuovo processo** ed eseguire i prossimi tre passi.



Crea nuovo processo

1. Cliccare nelle caselle per selezionare le partizioni, directory o file dei quali eseguire il backup.

   Quando selezionate un elemento nella parte sinistra della finestra, il suo contenuto verrà mostrato nella parte destra per aiutarvi a raffinare la vostra selezione.
2. Inserire un nome per il vostro lavoro di backup oppure accettare il nome lavoro predefinito.

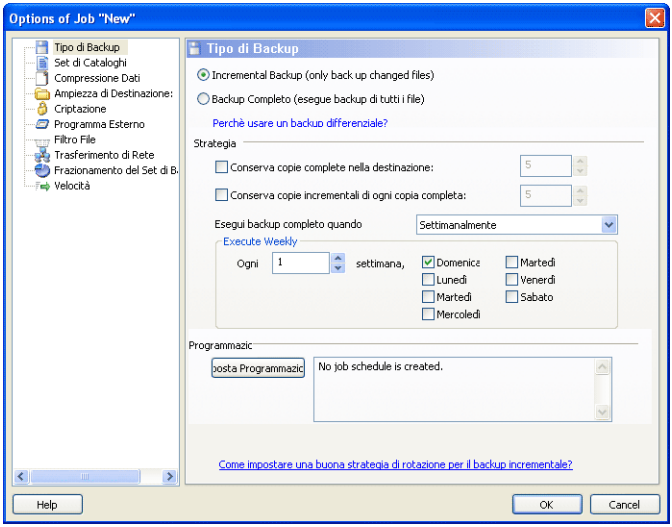
   Quando i file o directory vengono selezionati per il backup, automaticamente si genera un nome lavoro predefinito, ma esso può essere modificato.
3. Cliccare **Sfoglia** per scegliere dove salvare il vostro lavoro di backup.

Nota

Non dimenticare di cliccare su **Backup** per iniziare oppure su **Cancellare** per fermare il lavoro.
Per raffinare le vostre impostazioni, cliccare su **Opzioni**.

Finestra di dialogo Opzioni di Backup

Ci sono diverse sotto-opzioni nella finestra **Opzioni**.



Finestra di dialogo Opzioni di Backup

Tipo di Backup

Backup BitDefender supporta due tipi di backup.

- **Backup completo:** Esegue il backup completo di tutti i dati in origine al set di backup verso la destinazione specificata, Quando si esegue il backup completo, Backup BitDefender non farà il backup solo dei dati modificati ma di tutta l'origine dei dati.
- **Backup Incrementale:** La prima volta che viene eseguito, il Backup incrementale è uguale al completo in quanto esegue il backup completo di tutti i dati in origine verso il set di backup nella destinazione specificata. Più tardi, esso salverà solo i file creati o modificati di recente. Ogni volta che viene eseguito un backup incrementale viene creato anche un set di cataloghi di backup.

I backup completo ed incrementale possono essere combinati in un **Backup a Rotazione**. Per esempio, potete impostare un backup incrementale del lavoro, mentre impostate un backup completo una volta a la settimana, diciamo la domenica. Verrebbe fatto così: Selezionare **Settimanalmente** nel menu a tendina, 1 nel campo **Ogni settimana** e selezionare Domenica. Questo Backup completo della domenica sostituirà tutti i backup precedenti e sarà la base dalla quale partirà il Backup incrementale.

Set di Cataloghi

Si utilizza per avere un indice dell'informazione sui file di ogni backup, ed è la base del Backup incrementale e del processo di Ripristino. Il set di cataloghi

(*.ecs) contiene una serie di cataloghi che rappresentano un indice di tutti i file e directory nel set di backup. Tale indice include dati sulla data di backup, directory del backup, nome file e proprietà. I dati possono essere ripristinati dal set di cataloghi.

Un nome file per il set di cataloghi viene generato automaticamente dalla destinazione del lavoro. Per modificare il set di cataloghi di un lavoro, fare come segue:

1. Cliccare su **Set di Cataloghi** .
2. Inserire il nome del file nel campo corrispondente.
3. Cliccare su **Sfoglia** per selezionare la directory dove salvare i file del Set di cataloghi.
4. Selezionare **OK**.

Compressione Dati

Backup BitDefender permette la compressione ed il salvataggio dei dati nel set di backup per il risparmio di spazio durante l'esecuzione del backup. Esso supporta la Compressione Veloce, Standard e la Compressione ad Alta Intensità. Ad esempio, per iniziare una compressione standard con grado e velocità di compressione medi, seguire questi passi:

1. Cliccare su **Compressione Dati**.
2. Cliccare su **Compressione Standard**.
3. Selezionare **OK**.

Ampiezza Destinazione

BitDefender Backup permette la distribuzione del set di backup su diverse destinazioni. In questo caso, anche se una certa destinazione non avrà sufficiente spazio libero, l'esecuzione del backup continuerà.

È possibile aggiungere una o più destinazioni per continuare il backup, modificarle o addirittura rimuoverle, in uno dei seguenti modi:

1. Cliccare su **Ampiezza Destinazione**.
2. Cliccare su **Aggiungere** per selezionare una nuova destinazione dove salvare i dati del backup.
3. Cliccare su **Modificare** per modificare la destinazione di backup selezionata.
4. Cliccare su **Eliminare** per eliminare la destinazione di backup selezionata.
5. Cliccare su **Eliminare Tutte** per eliminare tutte le destinazioni di backup.
6. Selezionare **OK**.

Criptare

Backup BitDefender mantiene più sicuri i dati del backup criptando i dati prima di salvare il backup nel set. Le impostazioni di sicurezza di un lavoro includono la protezione mediante password.

Per criptare i dati prima del backup, seguire questi passi:

1. Cliccare su **Criptare**.
2. Scegliere un tipo di criptografia dal menu a tendina.
3. Inserire la vostra password nel campo corrispondente.

4. Reinserire la vostra password nel campo corrispondente.
5. Selezionare **OK**.

Programma Esterno

Il lavoro può eseguire altri comandi prima o dopo il backup, e il comando può essere `.exe`, `.com` o `.bat`, o un tipo specifico di evento come "spegnere il computer una volta completato il backup".

Per eseguire il comando all'inizio del backup, seguire questi passi:

1. Cliccare su **Programma Esterno**
2. Selezionare l'opzione**Prima dell'Esecuzione del Lavoro**.
3. Cliccare su **Sfogliare** per selezionare i file di comando da eseguire.
4. Selezionare **OK**.

Per eseguire un comando dopo che il backup è terminato, seguire questi passi:

1. Cliccare su **Programma Esterno**
2. Selezionare l'opzione**Dopo l'Esecuzione del Lavoro**.
3. Cliccare su **Sfogliare** per selezionare i file di comando da eseguire.
4. O cliccare su **Spegnere il computer** quando il backup sarà terminato.
5. O cliccare su **Riavviare il computer** quando il backup sarà terminato.
6. O cliccare su **Sconnettere l'utente corrente** quando il backup sarà terminato.
7. Selezionare **OK**.

Nota

Se volete che la configurazione lavori anche in caso di backup fallito, selezionare la casella **Eseguire Applicazione Esterna anche se l'Esecuzione del lavoro è fallita**.

Filtro File

Backup BitDefender fornisce una potente funzione di filtraggio per escludere o includere file, tipi di file o directory specificati, per risparmiare spazio disponibile e incrementare la velocità del backup.

I tipi di file specificati possono essere filtrati seguendo questi passi:

1. Cliccare su **Filtro File**.
2. Cliccare su **Tipo di Filtro**.
3. Escludere o includere i tipi di file nella finestra di dialogo che appare, selezionando le opzioni **Includere solo i tipi di file selezionati** o **Escludere i tipi di file selezionati**.
4. Se necessario, inserire un altro tipo di file nel campo **Personalizzare tipo** ma assicuratevi di utilizzare il formato `.abc`. Usare `,` (virgola) come separatore quando inserite più di un tipo personalizzato. Aggiungere una breve descrizione nel campo corrispondente.
5. Selezionare **OK**.

I file specificati possono essere filtrati seguendo questi passi:

1. Cliccare su **Filtro File**.

2. Cliccare su **Filtro File**.
3. Escludere o includere i file specifici nella finestra di dialogo che appare, selezionando le opzioni **Includere solo i file specificati dalla regola** o **Escludere i file specificati dalla regola**.
4. Cliccare su **Sfoglia** e selezionare il file. Il percorso all'ubicazione del file verrà aggiunto automaticamente nel campo **Applicato alle seguenti directory**. Per includere o escludere il file non corrispondente alla sua ubicazione, cliccare su **Applicato a tutte le directory**.
5. Selezionare **OK**.

La directory specificata può essere filtrata seguendo questi passi:

1. Cliccare su **Filtro File**.
2. Cliccare su **Filtrare Directory**.
3. Escludere o includere directory specifiche nella finestra di dialogo che appare, selezionando le opzioni **Includere solo le directory specificate dalla regola** o **Escludere le directory specificate dalla regola**.
4. Cliccare su **Sfoglia** e selezionare la directory. Il percorso all'ubicazione della directory verrà aggiunto automaticamente nel campo **Applicato alle seguenti directory**. Per includere o escludere directory non corrispondenti alle loro ubicazioni, cliccare su **Applicato a tutte le directory**.
5. Selezionare **OK**.

I filtri possono essere modificati seguendo questi passi:

1. Cliccare su **Filtro File**.
2. Cliccare sul filtro che desiderate modificare e quindi su **Modificare**.
3. Modificare le vostre opzioni nella finestra di dialogo.
4. Selezionare **OK**.

I filtri possono essere eliminati seguendo questi passi:

1. Cliccare su **Filtro File**.
2. Cliccare sul filtro che desiderate rimuovere e quindi su **Eliminare**.
3. O cliccare direttamente su **Eliminare Tutti**, per eliminare tutti i filtri.
4. Selezionare **OK**.

Trasferimento Rete

Backup BitDefender permette di eseguire accuratamente il backup ed il recupero di dati condivisi da gruppi di lavoro in rete. Se la rete non è accessibile riproverà ad effettuare il backup dei dati di volta in volta. per specificare la frequenza e quante volte riprovare a fare il backup, seguire questi passi.

1. Cliccare su**Trasferimento Rete**.
2. Cliccare su **In caso di mancata lettura di file in rete a causa di disconnessione, provare a riconnettere**.
3. Digitare la frequenza con cui volete ritentare il backup dei dati (in secondi).
4. Digitare quante volte ritentare il backup.
5. Selezionare **OK**.

Nota

Per evitare di essere travolti dalle informazioni sugli errori di rete, cliccare su **Nessun report di errore verrà generato quando la rete non è disponibile**.

Frazionamento del Set di Backup

Il set di backup generato può essere frazionato in molti altri set di backup, in modo che il backup possa essere eseguito normalmente anche quando la destinazione o file system sono limitati. Backup BitDefender fornisce due metodi di frazionamento: auto-split e sized-split.

Le impostazioni di frazionamento del backup del lavoro possono essere modificate come segue:

1. Cliccare su **Frazionamento del Set di Backup**.
2. Selezionare **Frazionamento Automatico in base allo Spazio nella Destinazione**.
3. O selezionare **Specificare la dimensione di frazionamento** e scegliere la dimensione desiderata dal menu a tendina.
4. Selezionare **OK**.

Velocità

Backup BitDefender supporta tre tipi di velocità. Più alta è la velocità, più CPU verrà utilizzata.

La velocità di Backup può essere specificata seguendo questi passi.

1. Cliccare su **Velocità**
2. Selezionare velocità **Massima**, **Media** o **Minima**.
3. Selezionare **OK**.

Verifica Dati

Per assicurarsi che i dati del vostro backup siano sempre sicuri, seguire questi passi.

1. Cliccare su **Verifica Dati**.
2. Cliccare su **Verificare i dati durante il processo di backup**.
3. Selezionare **OK**.

Processo di backup

Una volta che il lavoro è stato creato il backup viene automaticamente eseguito. Tuttavia, potete accedere a **Gestione Lavori** per eseguire il backup selezionando il lavoro creato e cliccando su **Lavoro di Backup** nel menu.

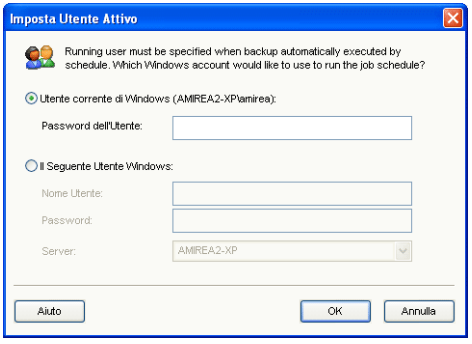
Per ricevere i dettagli del backup durante il recupero dei file, è necessario inserire una breve descrizione nel pop-up che si apre. Fare clic su **Annulla** per ignorare il pop-up oppure **OK** per continuare. Il processo di backup può essere anche cancellato facendo clic sul pulsante **Annulla backup**.

Nota

Per informazioni dettagliate, una buona idea sarebbe vedere **Proprietà**, **Report** e **Informazione su Esecuzione** del lavoro dalla finestra della barra di stato.

Programma processo

Qui potete programmare il lavoro di backup nel momento più oppurtuno.Potete programmare il lavoro affinchè sia eseguito giornalmente, settimanalmente, mensilmente o in qualsiasi momento specificato (per esempio all'avvio del sistema). **Programmare lavoro** è la base del backup automatico.



Programma processo

Se il vostro computer è membro di una rete di dominio, saranno necessari una serie di passi extra per aggiungere un programmatore di lavoro.

1. selezionare il lavoro e quindi cliccare su **Programmare Lavoro**.
2. Apparirà la finestra di dialogo **Utente Attivo**. Se voi siete l'utente di dominio, vi preghiamo di inserire la password di dominio.
3. Altrimenti selezionare **Eseguire come il seguente utente di Windows**.
4. Inserire il nome utente, la password ed il nome del server di dominio.
5. Selezionare **OK**.

Una volta che avete impostato l'utente attivo, Backup BitDefender mostrerà la finestra **Programmazione** in modo che potrete impostare un momento opportuno per eseguire il lavoro.

Qui potete specificare la frequenza con cui i compiti programmati verranno eseguiti: giornalmente, settimanalmente, mensilmente, una volta, all'avvio del sistema, all'accesso, quando il computer è ozioso. Se il compito è programmato giornalmente, settimanalmente, mensilmente, o una sola volta, potete anche specificare la data/ora di inizio. Potete selezionare anche la frequenza con cui il compito programmato verrà eseguito (espresso in numero di giorni o settimane, il giorno del mese o la

data). Un'altra possibile impostazione sarebbe la durata (in minuti) del periodo di ozio dopo il quale il compito programmato verrà iniziato.

È anche possibile configurare programmazioni multiple per un'attività facendo clic su **Mostra programmazioni multiple**. Facendo clic su **Avanzate** è possibile impostare opzioni di programmazione addizionali. Per esempio, si può definire la data di inizio e di fine dell'attività.

Per definire ulteriormente la programmazione del processo, fare clic sul pulsante **Impostazioni**. Ci sono tre sub-opzioni disponibili.

- **Funzione programmata completata**
  - Eliminare il compito se non è programmato per essere eseguito di nuovo.

    Questa funzione è utile per i compiti programmati per essere eseguiti solo una volta.
  - Fermare il compito se è in fase di esecuzione da:

    Specificare dopo quanto tempo dal suo inizio, il compito dovrebbe essere fermato.
- **Tempi Morti**
  - Iniziare il compito solo se il computer è stato ozioso per almeno:

    Specificare quanto tempo (in minuti) deve trascorrere senza uso del mouse o della tastiera prima che inizi il compito programmato.
  - Se il computer non è stato ozioso per così tanto, riprovare fino a:

    Specificare per quanto tempo (in minuti) il compito dovrà continuare a controllare se il computer è ozioso.
  - Fermare il compito se il computer smette di essere ozioso.

    Specificare se il compito si dovrà fermare nel caso in cui voi iniziate ad usare il computer mentre esso è in esecuzione.
- **Gestione Alimentazione**
  - Non iniziare il lavoro se il computer sta funzionando con le batterie.

    Specificare se si dovrebbe evitare di iniziare il compito nel caso in cui il vostro computer sta funzionando con le batterie. Selezionando questa casella potrete prolungare la vita delle vostre batterie.
  - Fermare il compito se inizia la modalità batteria.

    Specificare se il compito dovrebbe essere fermato nel caso in cui il vostro computer inizi a funzionare con le batterie.
  - Riattivare il computer per eseguire questo compito.

    Specificare se il computer dovrebbe eseguire il compito programmato anche quando è in sospensione.

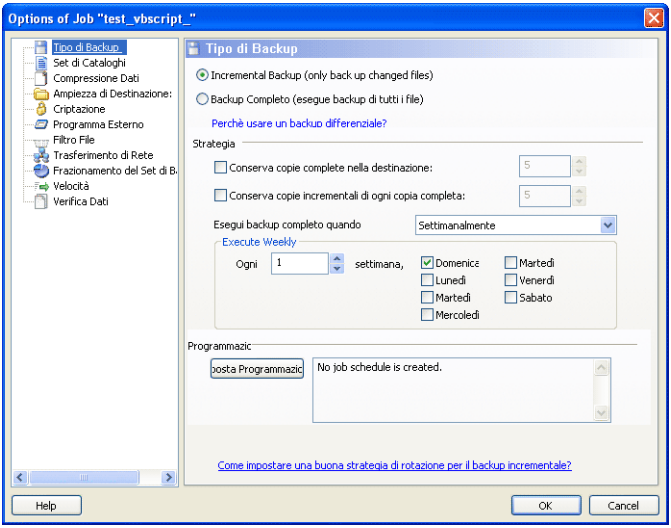
Elimina Programma processo

Per eliminare la programmazione di un lavoro, selezionarla e quindi cliccare su **Eliminare Programazione Lavoro** nella sezione **Gestione Lavori**.

Se il lavoro non è stato programmato, **Eliminare Programazione Lavoro** verrà mostrato in grigio, il che significa che non è utilizzabile.

Modifica Opzioni del processo

Per modificare le opzioni di un lavoro, selezionarlo e quindi cliccare su **Modificare Opzioni Lavoro** nella sezione **Gestione Lavori**.



Modifica Opzioni del processo

Il processo selezionato può essere un processo di backup o di masterizzazione.

Per ulteriori informazioni su come modificare i lavori di backup, fare riferimento a «*Finestra di dialogo Opzioni di Backup*» (p. 287).

Vediamo come è possibile modificare le opzioni di un processo di masterizzazione.

Modificare le Opzioni di un Lavoro di Masterizzazione

Ci sono diverse sub-opzioni disponibili nella finestra di dialogo del lavoro di masterizzazione.

Masterizzazione

Qui potete impostare se il disco deve essere espulso dopo la masterizzazione, finalizzato (se programmate di condividerlo con gli altri) oppure scritto usando il Joliet file system (meno restrizioni del nome file).

Se volete programmare il lavoro, cliccare su **Impostare Programmazione**.

Qui potete programmare il lavoro di backup nel momento più oppurtuno.Potete programmare il lavoro affinchè sia eseguito giornalmente, settimanalmente, mensilmente o in qualsiasi momento specificato (per esempio all'avvio del sistema). **Programmare lavoro** è la base del backup automatico.

Se il vostro computer è membro di una rete di dominio, saranno necessari una serie di passi extra per aggiungere un programmatore di lavoro.

1. selezionare il lavoro e quindi cliccare su **Programmare Lavoro**.
2. Apparirà la finestra di dialogo **Utente Attivo**. Se voi siete l'utente di dominio, vi preghiamo di inserire la password di dominio.
3. Altrimenti selezionare **Eseguire come il seguente utente di Windows**.
4. Inserire il nome utente, la password ed il nome del server di dominio.
5. Selezionare **OK**.

Una volta che avete impostato l'utente attivo, Backup BitDefender mostrerà la finestra **Programmazione** in modo che potrete impostare un momento opportuno per eseguire il lavoro.

Qui potete specificare la frequenza con cui i compiti programmati verranno eseguiti: giornalmente, settimanalmente, mensilmente, una volta, all'avvio del sistema, all'accesso, quando il computer è ozioso. Se il compito è programmato giornalmente, settimanalmente, mensilmente, o una sola volta, potete anche specificare la data/ora di inizio. Potete selezionare anche la frequenza con cui il compito programmato verrà eseguito (espresso in numero di giorni o settimane, il giorno del mese o la data). Un'altra possibile impostazione sarebbe la durata (in minuti) del periodo di ozio dopo il quale il compito programmato verrà iniziato.

È anche possibile configurare programmazioni multiple per un'attività facendo clic su **Mostra programmazioni multiple**. Facendo clic su **Avanzate** è possibile impostare opzioni di programmazione addizionali. Per esempio, si può definire la data di inizio e di fine dell'attività.

Per definire ulteriormente la programmazione del processo, fare clic sul pulsante **Impostazioni**. Ci sono tre sub-opzioni disponibili.

- **Funzione programmata completata**
  - Eliminare il compito se non è programmato per essere eseguito di nuovo.

    Questa funzione è utile per i compiti programmati per essere eseguiti solo una volta.
  - Fermare il compito se è in fase di esecuzione da:

Specificare dopo quanto tempo dal suo inizio, il compito dovrebbe essere fermato.

- **Tempi Morti**
  - Iniziare il compito solo se il computer è stato ozioso per almeno:

    Specificare quanto tempo (in minuti) deve trascorrere senza uso del mouse o della tastiera prima che inizi il compito programmato.
  - Se il computer non è stato ozioso per così tanto, riprovare fino a:

    Specificare per quanto tempo (in minuti) il compito dovrà continuare a controllare se il computer è ozioso.
  - Fermare il compito se il computer smette di essere ozioso.

    Specificare se il compito si dovrà fermare nel caso in cui voi iniziate ad usare il computer mentre esso è in esecuzione.
- **Gestione Alimentazione**
  - Non iniziare il lavoro se il computer sta funzionando con le batterie.

    Specificare se si dovrebbe evitare di iniziare il compito nel caso in cui il vostro computer sta funzionando con le batterie. Selezionando questa casella potrete prolungare la vita delle vostre batterie.
  - Fermare il compito se inizia la modalità batteria.

    Specificare se il compito dovrebbe essere fermato nel caso in cui il vostro computer inizi a funzionare con le batterie.
  - Riattivare il computer per eseguire questo compito.

    Specificare se il computer dovrebbe eseguire il compito programmato anche quando è in sospensione.

Programma Esterno

Il lavoro può eseguire altri comandi prima o dopo il backup, e il comando può essere `.exe`, `.com` o `.bat`, o un tipo specifico di evento come "spegnere il computer una volta completato il backup".

Per eseguire il comando all'inizio del backup, seguire questi passi:

1. Cliccare su **Programma Esterno**
2. Selezionare l'opzione**Prima dell'Esecuzione del Lavoro**.
3. Cliccare su **Sfogliare** per selezionare i file di comando da eseguire.
4. Selezionare **OK**.

Per eseguire un comando dopo che il backup è terminato, seguire questi passi:

1. Cliccare su **Programma Esterno**
2. Selezionare l'opzione**Dopo l'Esecuzione del Lavoro**.
3. Cliccare su **Sfogliare** per selezionare i file di comando da eseguire.
4. O cliccare su **Spegnere il computer** quando il backup sarà terminato.
5. O cliccare su **Riavviare il computer** quando il backup sarà terminato.
6. O cliccare su **Sconnettere l'utente corrente** quando il backup sarà terminato.

7. Selezionare **OK**.

Nota

Se volete che la configurazione lavori anche in caso di backup fallito, selezionare la casella **Eseguire Applicazione Esterna anche se l'Esecuzione del lavoro è fallita**.

Filtro File

Backup BitDefender fornisce una potente funzione di filtraggio per escludere o includere file, tipi di file o directory specificati, per risparmiare spazio disponibile e incrementare la velocità del backup.

I tipi di file specificati possono essere filtrati seguendo questi passi:

1. Cliccare su **Filtro File**.
2. Cliccare su **Tipo di Filtro**.
3. Escludere o includere i tipi di file nella finestra di dialogo che appare, selezionando le opzioni **Includere solo i tipi di file selezionati** o **Escludere i tipi di file selezionati**.
4. Se necessario, inserire un altro tipo di file nel campo **Personalizzare tipo** ma assicuratevi di utilizzare il formato `.abc`. Usare `,` (virgola) come separatore quando inserite più di un tipo personalizzato. Aggiungere una breve descrizione nel campo corrispondente.
5. Selezionare **OK**.

I file specificati possono essere filtrati seguendo questi passi:

1. Cliccare su **Filtro File**.
2. Cliccare su **Filtro File**.
3. Escludere o includere i file specifici nella finestra di dialogo che appare, selezionando le opzioni **Includere solo i file specificati dalla regola** o **Escludere i file specificati dalla regola**.
4. Cliccare su **Sfoglia** e selezionare il file. Il percorso all'ubicazione del file verrà aggiunto automaticamente nel campo **Applicato alle seguenti directory**. Per includere o escludere il file non corrispondente alla sua ubicazione, cliccare su **Applicato a tutte le directory**.
5. Selezionare **OK**.

La directory specificata può essere filtrata seguendo questi passi:

1. Cliccare su **Filtro File**.
2. Cliccare su **Filtrare Directory**.
3. Escludere o includere directory specifiche nella finestra di dialogo che appare, selezionando le opzioni **Includere solo le directory specificate dalla regola** o **Escludere le directory specificate dalla regola**.
4. Cliccare su **Sfoglia** e selezionare la directory. Il percorso all'ubicazione della directory verrà aggiunto automaticamente nel campo **Applicato alle seguenti directory**. Per includere o escludere directory non corrispondenti alle loro ubicazioni, cliccare su **Applicato a tutte le directory**.

5. Selezionare **OK**.

I filtri possono essere modificati seguendo questi passi:
1. Cliccare su **Filtro File**.
2. Cliccare sul filtro che desiderate modificare e quindi su **Modificare**.
3. Modificare le vostre opzioni nella finestra di dialogo.
4. Selezionare **OK**.

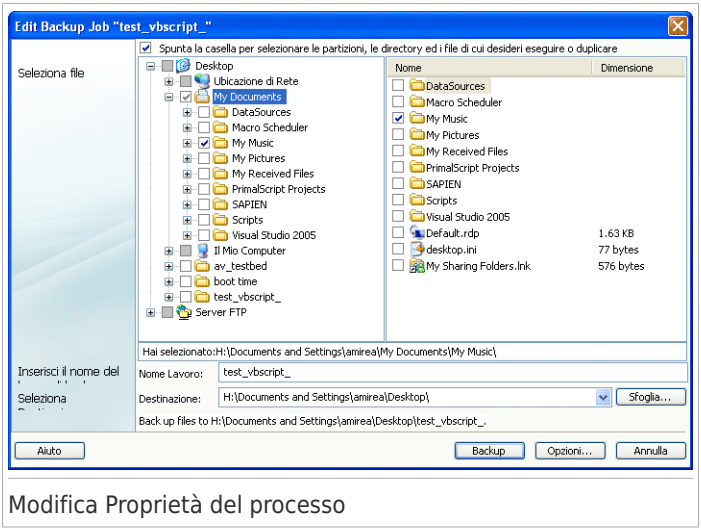
I filtri possono essere eliminati seguendo questi passi:
1. Cliccare su **Filtro File**.
2. Cliccare sul filtro che desiderate rimuovere e quindi su **Eliminare**.
3. O cliccare direttamente su **Eliminare Tutti**, per eliminare tutti i filtri.
4. Selezionare **OK**.

Verifica Dati

Per assicurarsi che i dati del vostro backup siano sempre sicuri, seguire questi passi.
1. Cliccare su **Verifica Dati**.
2. Cliccare su **Verificare i dati durante il processo di backup**.
3. Selezionare **OK**.

Modifica Proprietà del processo

Per modificare le proprietà di un lavoro, selezionare il lavoro interessato e quindi cliccare **Modificare Proprietà del Lavoro** nella sezione **Gestione Lavori**.



Modifica Proprietà del processo

1. Cliccare nelle caselle per selezionare le partizioni, directory o file dei quali eseguire il backup.

Quando selezionate un elemento nella parte sinistra della finestra, il suo contenuto verrà mostrato nella parte destra per aiutarvi a raffinare la vostra selezione.

2. Inserire un nome per il vostro lavoro di backup oppure accettare il nome lavoro predefinito.

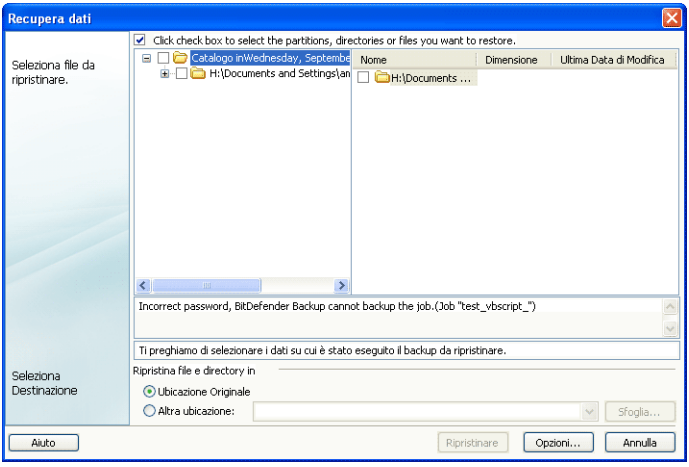
   Quando i file o directory vengono selezionati per il backup, automaticamente si genera un nome lavoro predefinito, ma esso può essere modificato.
3. Cliccare **Sfoglia** per scegliere dove salvare il vostro lavoro di backup.

Nota

Non dimenticare di cliccare su **Backup** per iniziare oppure su **Cancellare** per fermare il lavoro.
Per raffinare le vostre impostazioni, cliccare su **Opzioni**.

Recupera File

Per ripristinare i vostri dati dal backup, selezionare il lavoro dal quale volete ripristinare i dati, cliccare su **Ripristinare File** nel menu **Ripristino Lavori** e quindi seguire questi passaggi.



Recupera File

1. Selezionare le caselle accanto alle partizioni, directory o file da ripristinare.

   Quando selezionate un elemento nella parte sinistra della finestra, il suo contenuto verrà mostrato nella parte destra per aiutarvi a raffinare la selezione.
2. Nella finestra **Selezionare Ubicazione di Ripristino**, potete usare l'ubicazione originale senza nessun cambio oppure specificare un'altra ubicazione dove ripristinare il file.

Cliccare **Sfoglia** per scegliere dove salvare il vostro lavoro di backup.

Nota
Non dimenticare di cliccare su **Ripristinare** per iniziare oppure **Cancellare** per fermare il processo.
Per raffinare le vostre impostazioni, cliccare su **Opzioni**.

Finestra di dialogo delle Opzioni di Ripristino

Le opzioni di ripristino permettono di specificare se i file da ripristinare esistono già nella destinazione nel momento del ripristino, e se aggiornare la data di modifica di ogni file ripristinato.

Quando i file da ripristinare esistono già

- **Ignora file** BitDefender ignora i relativi file.
- **Chiedere all'utente se sostituire o meno i file** BitDefender chiede se sostituire o meno i file già esistenti.
- **Sostituisci sempre i file direttamente** BitDefender sostituisce i file senza chiedere il consenso.
- **Sostituire solo i file più vecchi dei file di backup** BitDefender sostituisce solo i file più vecchi. I file più vecchi vengono determinati dalla data in cui sono stati modificati.

Data di Modifica del File

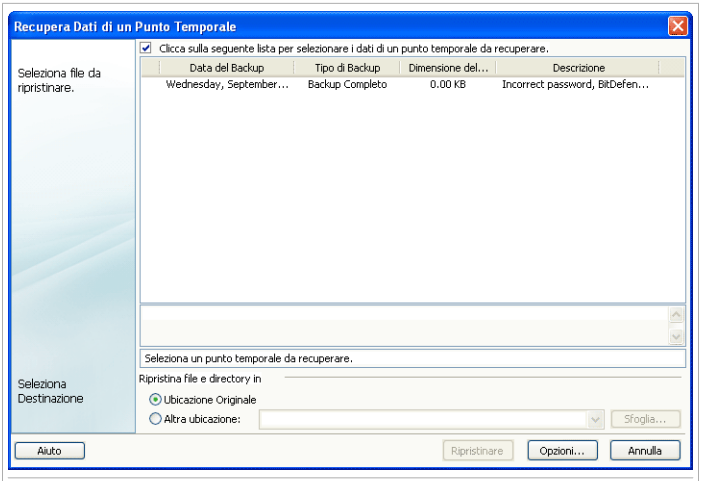
Se l'opzione è selezionata, BitDefender utilizza la data corrente per indicare la data in cui i file e le directory sono stati ripristinati. Se no, BitDefender utilizzerà come data di modifica del file o directory quella in cui è stato eseguito il backup.

Struttura della Directory

Diventa attiva solo se scegliete di ripristinare i dati in un'altra directory. Potete anche conservare la struttura di directory dei vostri dati.

Recupera Dati di un Punto Temporale

Per ripristinare i dati su cui avete eseguito il backup in un punto temporale specifico, selezionare il lavoro dal quale volete recuperare i dati, cliccare su **Ripristinare dati di un punto temporale** nel menu **Ripristino Lavoro** e quindi seguire questi passaggi.



Ripristinare dati di un punto temporale

1. Selezionare dalla lista il set di backup di un punto temporale specificato. I commenti verranno mostrati sotto.
2. Nella finestra **Selezionare Ubicazione di Ripristino**, potete usare l'ubicazione originale, senza modifiche, o specificare un'altra ubicazione dove ripristinare il file.

   Cliccare **Sfoglia** per scegliere dove salvare il vostro lavoro di backup.

Nota
Non dimenticare di cliccare su **Ripristinare** per iniziare oppure **Cancellare** per fermare il processo.
Per raffinare le vostre impostazioni, cliccare su **Opzioni**.

Finestra di dialogo delle Opzioni di Ripristino

Le opzioni di ripristino permettono di specificare se i file da ripristinare esistono già nella destinazione nel momento del ripristino, e se aggiornare la data di modifica di ogni file ripristinato.

Quando i file da ripristinare esistono già

- **Sostituire solo i file più vecchi dei file di backup** BitDefender sostituisce solo i file più vecchi. I file più vecchi vengono determinati dalla data in cui sono stati modificati.

Data di Modifica del File

Se l'opzione è selezionata, BitDefender utilizza la data corrente per indicare la data in cui i file e le directory sono stati ripristinati. Se no, BitDefender utilizzerà come data di modifica del file o directory quella in cui è stato eseguito il backup.

Struttura della Directory

Diventa attiva solo se scegliete di ripristinare i dati in un'altra directory. Potete anche conservare la struttura di directory dei vostri dati.

Controllo Lavori

Ci sono tre modi di controllare un lavoro: sospendere, fermare e fermare tutti.

Pausa

Per sospendere un processo di backup o di recupero in corso, fare clic sul pulsante **Sospendi processo** nel menu **Controllo processi**.

Fermare

Per fermare un processo di backup o di recupero in corso, fare clic sul pulsante **Ferma processo** nel menu **Controllo processi**.

Fermare tutti

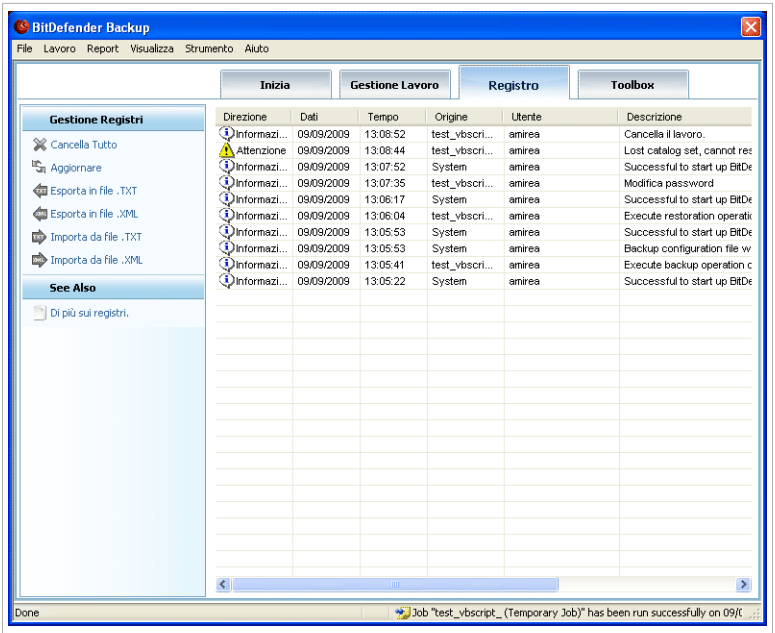
Se ci sono più di un processo di backup o di ripristino in corso, non è necessario fermarli uno ad uno. Fare clic sul pulsante **Ferma tutti** nel menu **Controllo processi** per fermarli tutti in una volta sola.

24.1.3. Registro

Questa sezione vi mostra come visualizzare, importare, esportare e cancellare i registri. L'opzione Registro vi permette di ricordare quello che avete salvato mediante backup e ripristinato e quando lo avete fatto, e vi mostra anche gli avvisi o gli errori nelle operazioni. Per esempio, se si verifica un errore di lettura di un file durante l'esecuzione, BitDefenser lo registrerà come un messaggio di avviso.

Potete passare a **Visualizzatore di Registro** faccendo come segue:

- Cliccare su **Visualizzatore di Registro** nella **Barra di Navigazione**.
- Cliccare su **Visualizzare** nella **Barra di Menu** e selezionare **Visualizzatore di Registro**.
- Utilizzare un collegamento premendo **CTRL+Alt+L**.


BitDefender Backup
File Lavoro Report Visualizza Strumento Aiuto
Inizia
Gestione Lavoro
Registro
Toolbox
Gestione Registri
Cancella Tutto
Aggiornare
Esporta in file .TXT
Esporta in file .XML
Importa da file .TXT
Importa da file .XML
See Also
Di più sui registri.
Direzione Dati Tempo Origine Utente Descrizione
Informazi... 09/09/2009 13:08:52 test_vbscri... amirea Cancella il lavoro.
Attenzione 09/09/2009 13:08:44 test_vbscri... amirea Lost catalog set, cannot res
Informazi... 09/09/2009 13:07:52 System amirea Successful to start up BitDe
Informazi... 09/09/2009 13:07:35 test_vbscri... amirea Modifica password
Informazi... 09/09/2009 13:06:17 System amirea Successful to start up BitDe
Informazi... 09/09/2009 13:06:04 test_vbscri... amirea Execute restoration operati
Informazi... 09/09/2009 13:05:53 System amirea Successful to start up BitDe
Informazi... 09/09/2009 13:05:53 System amirea Backup configuration file w
Informazi... 09/09/2009 13:05:41 test_vbscri... amirea Execute backup operation c
Informazi... 09/09/2009 13:05:22 System amirea Successful to start up BitDe
Done
Job "test_vbscript_ (Temporary Job)" has been run successfully on 09/(

Registro

Visualizza registri

L'opzione di visualizzazione dei registri vi permette di rintracciare la vostra operazione e scoprire la causa dell'errore nell'operazione.

La descrizione di un registro in Backup BitDefender contiene i seguenti elementi:

Tipo

Una classifica della severità del registro. Ci sono quattro gradi di severità in Backup BitDefender:

- **Fatale:** Un problema significativo che impedisce a Backup BitDefender di funzionare normalmente. Per esempio, il file di configurazione di Backup BitDefender è stato danneggiato.
- **Errore:** Un problema che conduce al fallimento di un'operazione. Per esempio, è stato eseguito il backup di un lavoro su un server, ma il server è inaccessibile.
- **Avviso:** un problema che non colpisce un'operazione, ma può essere classificato più tardi come evento. Per esempio, un file non può essere letto nel processo di backup.
- **Informazione:** Descrive un'operazione eseguita con successo. Per esempio, un lavoro è stato eliminato con successo.

Data
La data in cui l'oggetto del registro è accaduto.

Ora
L'ora locale in cui l'oggetto del registro è accaduto.

Origine
L'origine del registro dell'oggetto, il quale può essere un lavoro oppure l'applicazione Backup BitDefender. Per esempio, un oggetto con il commento System indica che esso è stato generato dalla l'applicazione Backup BitDefender. Altri possibili commenti sono i nomi dei processi di Backup BitDefender che abbianno registrato i relativi elementi.

Utente
Il nome del utente la cui azione ha generato il registro dell'oggetto.

Descrizione
Presenta il contenuto dettagliato dell'oggetto registrato.

Pulisci registro (log)

Backup BitDefender fornisce due modi per cancellare i registri: automaticamente e manualmente.

Importante
Una volta che il registro è stato cancellato, non può essere più recuperato. Per ciò, è meglio esportare tutti i registri in un file e conservarli per consultazioni future.

Cancellare Automaticamente
All'inizio di Backup BitDefender, appare la dimensione di registro esistente come dimensione predefinita, Backup BitDefender cancellerà automaticamente tutti i file di registro che eccedano la dimensione predefinita.

Nota
Per scoprire o modificare la dimensione predefinita di registro, seguire questi passi:
1. Cliccare su **Strumenti** nella **Barra di Menu**.
2. Cliccare su **Opzioni** e quindi selezionare **Report e Registro**.
3. Inserire il limite di dimensione desiderato (in MB) nel campo corrispondente. Quando la dimensione del registro raggiungerà questo limite, Backup BitDefender cancellerà tutti i registri.

Cancellare Manualmente
Seguire questi passi per cancellare i registri manualmente.
1. Cliccare su **Cancella Tutti** nel menu **Gestione Registri**.
2. Fare clic su **OK** per esportare certi registri prima di cancellarli, o fare clic su **No** se non si vuole conservare i registri.

Importare ed Esportare Registri

Backup BitDefender supporta attualmente l'importazione ed esportazione di file in due formati: `.TXT` e `.XML`

Nota
Vi consigliamo di esportare e salvare il registro in un file prima di cancellarlo.

Per esportare i registri in un file specifico, seguire questi passi:

1. Fare clic su **Esporta in file .TXT** o **Esporta in file .XML** nel menu **Gestione registri**.
2. Inserire il nome file e scegliere l'ubicazione dove salvare il vostro file.
3. Cliccare su **Salvare**,

Per importare registri da un file specifico, seguire questi passi:

1. Fare clic su **Importa da file .TXT** o **Importa da file .XML** nel menu **Gestione registri**.
2. Trovare il vostro File.
3. Cliccare **Aprire**.

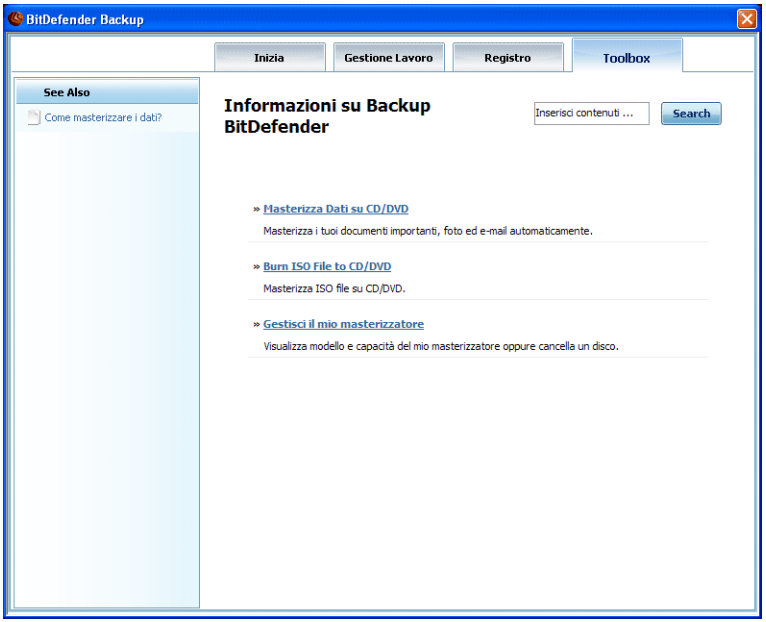
Nota
Fare clic sul pulsante **Aggiorna** nel menu **Gestione Registri** per assicurare di visualizzare i registri più recenti.

24.1.4. Toolbox

Questa sezione vi mostra come utilizzare Backup BitDefender per masterizzare dati su CD/DVD oppure masterizzare un file d'immagine ISO. Copre argomenti come la masterizzazione di CD-R/RW, DVD-R/RW/RAM, DVD+R/RW/DL e la conservazione fuori rete dei dati resultanti del backup.

Petete passare alla **Toolbox** facendo come segue:

- Cliccare su **Toolbox** nella **Barra di Navigazione**.
- Cliccare su **Visualizzare** nella **Barra di Menu** e selezionare **Toolbox**.
- Utilizzare il collegamento premendo **CTRL+Alt+T**.



Toolbox

Masterizzare su CD/DVD

Per masterizzare dati su CD/DVD manualmente, seguire questi passi:

1. Cliccare su **masterizzare dati su CD/DVD** .
2. Fare clic su **Cancella** se si vuole riutilizzare un disco riscrivibile. Se si desidera cancellarlo velocemente, fare clic su **Veloce**. Se è necessario cancellare completamente l'informazione registrata, fare clic su **Completa**, ma questo richiederà un po' di tempo.
3. Cliccare su **Masterizzare con dialogo**.

   Qui potete impostare se il disco deve essere espulso dopo la masterizzazione, finalizzato (se programmate di condividerlo con gli altri) oppure scritto usando il Joliet file system (meno restrizioni del nome file).
4. Cliccare su **File** or**Directory** nella finestra di dialogo che appare per aggiungere dati che volete masterizzare.
5. Dopo che avete aggiunto i dati, selezionare il masterizzatore ed il nome del disco sul quale verranno masterizzati i dati, e quindi cliccare su **Masterizzare**.

Masterizzare File d'Immagine ISO su CD/DVD

Per masterizzare un file d'immagine ISO su CD/DVD, seguire questi passi:

1. Cliccare su **Masterizzare File d'Immagine ISO su CD/DVD**.
2. Fare clic su **Cancella** se si vuole riutilizzare un disco riscrivibile. Se si desidera cancellarlo velocemente, fare clic su **Veloce**. Se è necessario cancellare completamente l'informazione registrata, fare clic su **Completa**, ma questo richiederà un po' di tempo.
3. Cliccare su **Masterizzare con dialogo**.

   Qui potete impostare se il disco deve essere espulso dopo la masterizzazione, finalizzato (se programmate di condividerlo con gli altri) oppure scritto usando il sistema Joliet file (meno restrizioni del nome file).
4. Selezionare **Aggiungi**.
5. Scegliere un file d'immagine ISO da masterizzare e cliccare **OK**.
6. Cliccare su **Masterizzare**.

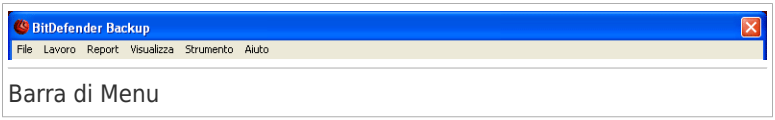
Gestisci il mio masterizzatore

Questo vi aiuta a gestire e visualizzare il dispositivo di registrazione ed i dischi nel sistema corrente. Contiene i seguenti links:

- **Eject** Apre il dispositivo di registrazione selezionato.
- **Chiudere** Chiude il dispositivo di registrazione selezionato.
- **Informazioni Media** Consente di visualizzare le informazioni Media del dispositivo di registrazione.
- **Informazioni Dispositivo** Consente di visualizzare le informazioni sul dispositivo di registrazione.
- **Potenzialità** Permette di visualizzare le potenzialità del dispositivo di registrazione.
- **Cancellare Media** Cancella i contenuti del disco.

24.1.5. Barra di Menu

Ci sono sei menu disponibili per eseguire tutte le funzioni offerte dalla soluzione di backup di BitDefender.



Barra di Menu

File

- **Creare Nuovo Lavoro:** Mostra una finestra di dialogo per creare un nuovo lavoro di backup o un altro lavoro.
- **Aprire Set di Backup:** Mostra una finestra di dialogo per aprire il set di backup o il set di cataloghi per il recupero.

- **Uscire:** Consente di uscire dalla sezione di backup di BitDefender.

Lavoro

- **Backup:** Esegue il backup del lavoro selezionato. Se c'è più di un lavoro selezionato, eseguirà il backup di tutti i lavori selezionati.
- **Ripristinare File:** Esegue il ripristino del lavoro selezionato. Se c'è più di un lavoro selezionato, eseguirà il ripristino di tutti i lavori selezionati.
- **Ripristinare Dati di un Punto temporale:** Recupera il lavoro selezionato in un certo punto temporale. Se c'è più di un lavoro selezionato, eseguirà il recupero di tutti i file selezionati.
- **Programmazione:** Crea la programmazione del lavoro o modifica l'esistente.
- **Eliminare Programmazione:** Cancella la programmazione del lavoro specificato.
- **Eliminare:** Elimina il lavoro selezionato. Se c'è più di un lavoro selezionato, eseguirà l'eliminazione di tutti i file selezionati.
- **Eliminare tutti:** - cancella tutti i lavori nella Gestione lavori.
- **Sfoglia Destinazione:** Permette visualizzare i dati di backup della destinazione del lavoro selezionato.
- **Modificare Opzioni:** Modifica le opzioni del lavoro selezionato.
- **Proprietà:** Permette di modificare le proprietà del lavoro selezionato, inclusi dati in origine, nome, destinazione, etc del lavoro.

Report

- **Visualizza Report:** Se il processo selezionato ha delle impostazioni di sicurezza, questa opzione permette di vedere i contenuti del report del processo.
- **Salvare come:** Salva i contenuti del report selezionato in un file specificato.
- **Stampare:** Stampa i contenuti del report selezionato .
- **Pulire tutto:** Cancella i contenuti del report del lavoro selezionato.
- **Aggiornare:** Aggiorna i contenuti del report del lavoro selezionato.

Visualizzare

- **Iniziare:** Se la finestra d'inizio non è stata ancora visualizzata, questa opzione permette di aprirla.
- **Gestione Lavori:** Se la finestra Gestione Lavori non è stata ancora visualizzata, questa opzione permette di aprirla.
- **Visualizzatore di Registro:** Se la finestra Visualizzatore di Registro non è stata ancora visualizzata, questa opzione permette di aprirla.
- **Toolbox:** Se la finestra non è stata ancora visualizzata, questa opzione permette di aprirla.
- **Mostrare Barra di Menu:** Nasconde la Barra di Menu. Per mostrarla, premere semplicemente **ALT**.
- **Mostrare Griglia:** Mostra o nasconde la griglia. Riguarda le finestre del visualizzatore di registro e della gestione lavori.

Strumento

- **Assistente di Backup:** Inizia la procedura di backup.
- **Assistente di Ripristino:** Inizia la procedura di ripristino.
- **Masterizzare:** avvia il masterizzatore CD/DVD/ISO o uno strumento di gestione di masterizzazione.
  - **Masterizzazione CD/DVD**
  - **Masterizzare File ISO**
  - **Visualizzare Infromazioni del Masterizzatore**
- **Esportare tutti i lavori:** Esporta tutti i lavori creati in un file specificato.
- **Importare Lavori:** Importa dei lavori da un file `.JOB`, `.TXT`, o `.XML`.
- **Esportare registri:** Esporta registri in un file `.TXT` o `.XML`.
  - In un file TXT
  - In un file XML
- **Importare registri:** Importa registri da un file `.TXT` o `.XML`.
  - Da un file TXT
  - Da un file XML
- **Opzioni:** Modifica le vostre opzioni globali di backup.
  - **Generale**
  - **Registro& report**
  - **Programmazione Lavoro**

Aiuto

- **Argomento di Aiuto** - Mostra argomenti di aiuto.
- **Cercare:** Permette di cercare argomenti di aiuto in base alle parole chiavi selezionate o inserite.
- **BitDefender nella Pagina web:** Permette di accedere alla homepage di BitDefender per guardare le notizie su BitDefender ed il supporto on line.
- **Informazioni di supporto:** fornisce informazioni su come contattare BitDefender per aiuto e supporto.
- **Informazioni su Backup BitDefender:** Mostra le informazioni relative al copyright, la versione e l'edizione di Backup BitDefender.

25. Criptazione

BitDefender offre delle capacità di criptazione per proteggere i vostri documenti confidenziali e le vostre conversazioni attraverso Yahoo Messenger e MSN Messenger.

25.1. Criptazione Chat (IM)

Di default, BitDefender esegue la criptazione di tutte le vostre sessioni chat, purché:

- Il tuo partner di chat abbia una versione di BitDefender installata che supporti la Criptazione Chat, e la Criptazione Chat sia abilitata per l'applicazione usata per chattare.
- Tu ed il tuo partner di chat usate entrambi Yahoo Messenger o Windows Live (MSN) Messenger.

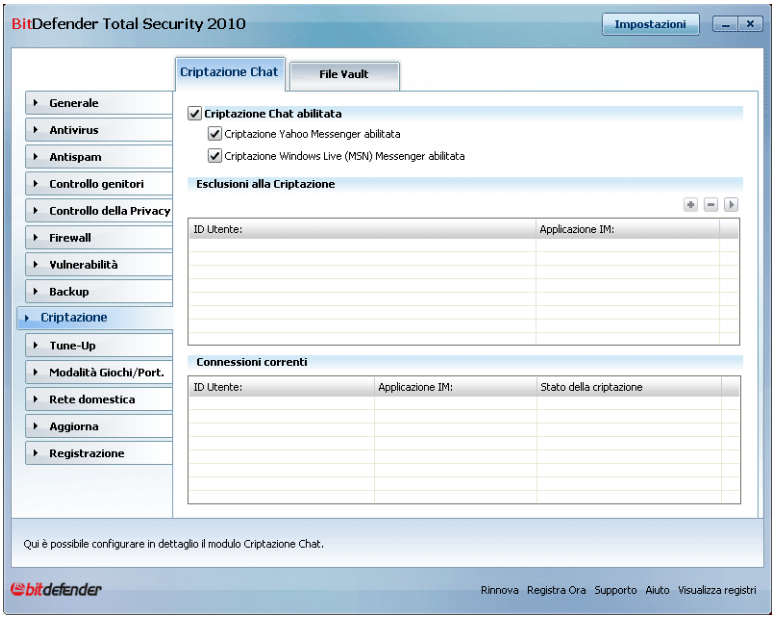
Importante

BitDefender non eseguirà la criptazione di una conversazione se uno dei partner utilizza un'applicazione chat su web, come Meebo, o se uno dei partner utilizza Yahoo! e l'altro Windows Live (MSN).

Per configurare la criptazione dell'instant messaging, fare clic su **Criptazione>Criptazione IM** in Modalità Avanzata.

Nota

Potete configurare facilmente la criptazione dell'instant messaging utilizzando la barra degli strumenti di BitDefender nella finestra di chat. Per ulteriori informazioni fare riferimento a «*Integrazione in Programmi Instant Messenger*» (p. 363).



Criptazione Chat

Di default, la Criptazione Chat è abilitata sia per Yahoo Messenger che per Windows Live (MSN) Messenger. Potete scegliere di disabilitare la Critazione Chat solo per una specifica applicazione di chat o completamente.

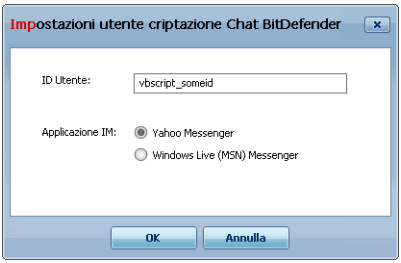
Vengono mostrate due tabelle:

- **Esclusioni della Criptazione** - elenca le ID degli utenti ed i relativi programmi di chat per i quali la criptazione è disabilitata. Per rimuovere un contatto dall'elenco, selezionarlo e quindi fare clic sul pulsante **Rimuovi**.
- **Connessioni Correnti** - elenca le connessioni in corso di chat (ID utente e programma associato) e se queste sono criptate o meno. Una connessione può non essere criptata per questi motivi:
  - Avete esplicitamente disabilitato la criptazione per questo contatto.
  - Il vostro contatto non ha installata una versione di BitDefender che supporti la Criptazione chat.

25.1.1. Disabilitare la Criptazione per Utenti Specifici

Per disabilitare la criptazione per uno specifico utente, seguire questi passaggi:

1. Fare clic sul pulsante **Aggiungi** per aprire la finestra di configurazione.



Aggiungere Contatti

2. Digitare la ID utente del vostro contatto nel campo corrispondente.
3. Selezionare l'applicazione di instant messaging associata al contatto.
4. Selezionare **OK**.

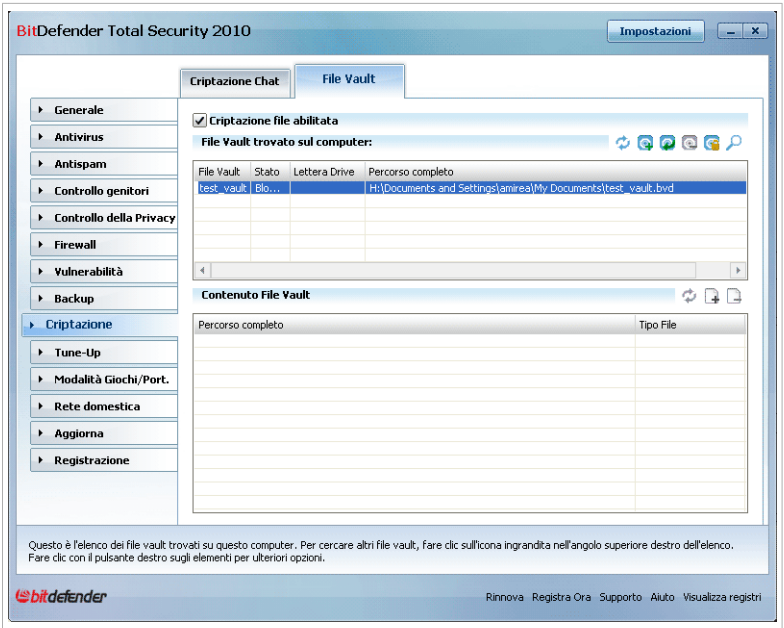
25.2. Criptazione file

La Criptazione File di BitDefender permette di creare dei drive logici (o vault) criptati e protetti da password sul computer, dove è possibile immagazzinare i documenti confidenziali e sensibili in modo sicuro. L'accesso ai dati immagazzinati in questi vault è consentito solo agli utenti che conoscono la password.

La password vi consente di aprire, immagazzinare dati e chiudere un vault mentre mantenete la sua sicurezza. Mentre un vault è aperto, potete aggiungere dei nuovi file, accedere ai file correnti o modificarli.

Fisicamente, il vault è un file immagazzinato nel disco rigido locale, con l'estensione `.bvd`. Anche se l'accesso ai file fisici che rappresentano i drive protetti è possibile da diversi sistemi operativi (come Linux), le informazioni immagazzinate in essi non possono essere lette perchè criptate.

Per gestire i file vault sul computer, fare clic su **Criptazione>Criptazione File** in Modalità Avanzata.



File Vault

Per disabilitare la Criptazione File, deselezionare la casella **Criptazione File abilitata** e fare clic su **Sì** per confermare. Se disabilitate la Criptazione File, tutti i vault verranno bloccati e non potrete più accedere ai file che li contengono.

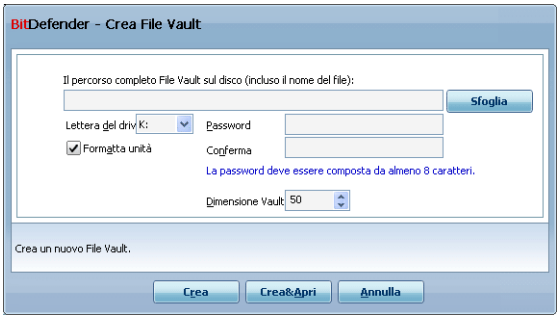
La tabella nella parte superiore mostra i vault sul vostro computer. Potete vedere il nome, lo stato (aperto/bloccato), la lettera del drive ed il percorso completo del vault. La tabella nella parte inferiore mostra il contenuto del vault selezionato.

25.2.1. Creare un Vault

Per creare un nuovo vault, utilizzare uno di questi metodi:

- Cliccare su **Creare vault**.
- Fare clic con il tasto destro nella tabella dei vault e selezionare **Crea**.
- Fare clic con il pulsante destro sul desktop o su una cartella del computer, puntare su **Criptazione File BitDefender** e selezionare **Crea**.

Apparirà una nuova finestra.



Crea File Vault

Procedere come segue:

1. Specificare la posizione ed il nome del vault.
   - Cliccare su **Sfoglia**, selezionare la posizione del vault e salvare il file sotto il nome desiderato.
   - È sufficiente digitare il nome del vault nel campo corrispondente per crearlo in Documenti. Per aprire i Documenti, fare clic su start menu Start di Windows e poi **Documenti**.
   - Digitare il percorso completo del vault sul disco. Ad esempio, `C:\my_vault.bvd`.
2. Scegliere una lettera dal menu per il drive. Quando aprite il vault, un disco virtuale con la lettera selezionata apparirà su Risorse del Computer.
3. Digitare la password desiderata per il vault nei campi **Password** e **Conferma**. Qualsiasi persona che tenti di aprire il vault ed accedere ai suoi file, dovrà fornire la password.
4. Selezionare **Formattare drive** per formattare il disco virtuale assegnato al vault. È necessario formattare l'unità prima che si possa aggiungere file al vault.
5. Se desiderate cambiare la dimensione predefinita del vault (50 MB), digitare il valore desiderato nel campo **Dimensione del Vault**.
6. Cliccare su **Creare** se desiderate creare solo il vault nella destinazione selezionata. Per creare e mostrare il vault come un disco virtuale nelle Risorse del Computer, cliccare su **Creare & Aprire** .

BitDefender informerà immediatamente sul risultato dell'operazione. Se si verifica un errore, utilizzare il messaggio di errore per risolvere l'errore. Selezionare **OK** per chiudere la finestra.

Nota
Potrebbe essere conveniente salvare tutti i file vault nella stessa posizione. In questo modo, è possibili trovarli più velocemente.

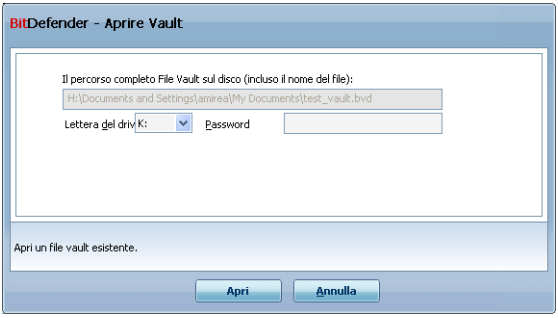
25.2.2. Aprire un Vault

Per accedere e lavorare sui file immagazzinati in un vault, dovrete aprire il vault. Quando aprite un vault, apparirà un disco virtuale nelle Risorse del Computer. Il drive avrà la lettera di disco assegnata al vault.

Per aprire un vault, utilizzare uno di questi metodi:

- Selezionare il vault dalla tabella e cliccare su **Aprire vault**.
- Fare clic con il pulsante destro sul vault nella tabella e selezionare **Apri**.
- Fare clic con il pulsante destro sul vault nel computer, puntare su **Criptazione File BitDefender** e selezionare **Apri**.

Apparirà una nuova finestra.



Aprire Vault

Procedere come segue:

1. Scegliere una lettera dal menu per il drive.
2. Digitare la password per il vault nel campo **Password**.
3. Cliccare **Aprire**.

BitDefender informerà immediatamente sul risultato dell'operazione. Se si verifica un errore, utilizzare il messaggio di errore per risolvere l'errore. Selezionare **OK** per chiudere la finestra.

25.2.3. Bloccare un Vault

Quando abbiate finito di lavorare in un vault, dovrete bloccarlo per proteggere i vostri dati. Bloccando la vault, l'unità disco virtuale corrispondente sparisce da

Risorse del computer. Di conseguenza l'accesso ai dati archiviati nel vault è completamente bloccato.

Per bloccare un vault, utilizzare uno di questi metodi:

- Selezionare il vault nella tabella e cliccare su **Bloccare vault**.
- Fare clic con il pulsante destro sul vault nella tabella e selezionare **Blocca**.
- Fare clic con il pulsante destro sul disco virtuale corrispondente da Risorse del Computer, puntare su **Criptazione File BitDefender** e selezionare **Blocca**.

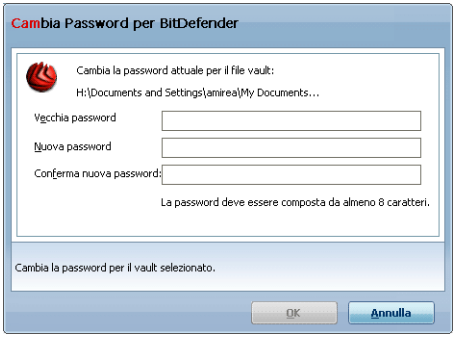
BitDefender informerà immediatamente sul risultato dell'operazione. Se si verifica un errore, utilizzare il messaggio di errore per risolvere l'errore. Selezionare **OK** per chiudere la finestra.

25.2.4. Cambiare la Password del Vault

Il vault deve essere bloccato prima che si possa cambiare la sua password. Per cambiare la password di un vault, utilizzare uno di questi metodi:

- Selezionare il vault nella tabella e cliccare su **Cambiare password**.
- Fare clic con il pulsante destro sul vault nella tabella e selezionare **Cambia password**.
- Fare clic con il pulsante destro sul vault sul computer, puntare su **Criptazione File BitDefender** e selezionare **Cambia la password del vault**.

Apparirà una nuova finestra.


Cambia Password per BitDefender
Cambia la password attuale per il file vault:
H:\Documents and Settings\amirea\My Documents...
Vecchia password
Nuova password
Conferma nuova password:
La password deve essere composta da almeno 8 caratteri.
Cambia la password per il vault selezionato.
OK
Annulla

Cambiare la Password del Vault

Procedere come segue:

1. Digitare la password corrente del vault nel campo **Vecchia password**.
2. Digitare la nuova password del vault nei campi **Nuova password** e **Confermare nuova password**.

Nota

La password deve essere composta da almeno 8 caratteri. Per avere una password forte, utilizzare una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @).

3. Cliccare su **OK** per cambiare la password.

BitDefender informerà immediatamente sul risultato dell'operazione. Se si verifica un errore, utilizzare il messaggio di errore per risolvere l'errore. Selezionare **OK** per chiudere la finestra.

25.2.5. Aggiungere dei File ad un Vault

Per aggiungere dei file ad un vault, seguire questi passaggi:

1. Seleziona dalla tabella vault il vault a cui si desidera aggiungere file.
2. Se il vault è bloccato, prima bisogna aprirlo (facendo clic con il pulsante destro e selezionando **Apri vault**).
3. Cliccare su **Aggiungere file**. Apparirà una nuova finestra.
4. Selezionare i file / cartelle che volete aggiungere al vault.
5. Cliccare **OK** per copiare gli oggetti selezionati nel vault.

Una volta che il vault è aperto, è possibile utilizzare direttamente l'unità disco virtuale corrispondente al vault. Attenersi alla seguente procedura:

1. Aprire Documenti (fare clic su start menu Start di Windows e poi **Risorse del computer**).
2. Inserire l'unità disco virtuale corrispondente al vault. Cercare la lettera dell'unità assegnata al vault quando lo si è aperto.
3. Copia e incolla e trascina file e cartelle direttamente a questa unità disco virtuale.

25.2.6. Rimuovere dei File da un Vault

Per rimuovere un file da un vault, seguire questi passaggi:

1. Selezionare dalla tabella dei vault quello contenente il file da rimuovere.
2. Se il vault è bloccato, prima bisogna aprirlo (facendo clic con il pulsante destro e selezionando **Apri vault**).
3. Selezionare il file da rimuovere dalla tabella che mostra il contenuto del vault.
4. Fare clic su **Elimina file/cartelle**.

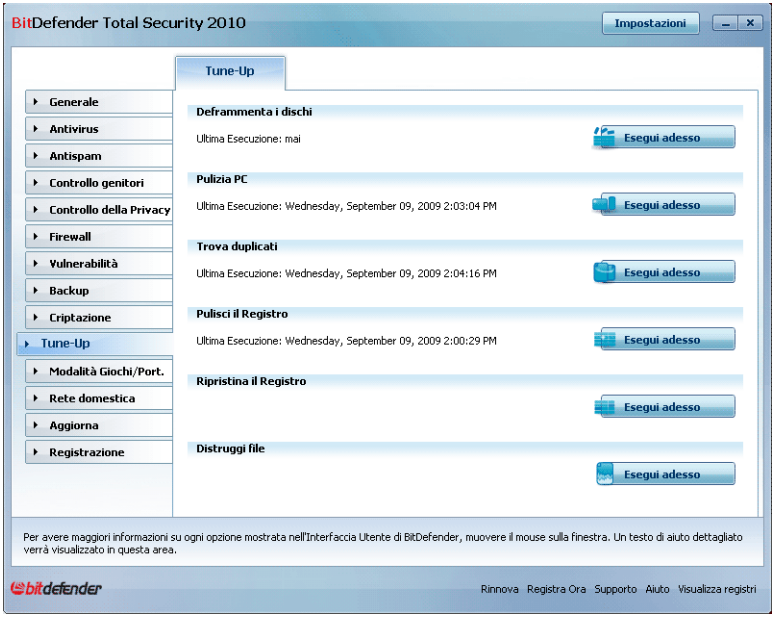
Se il vault è aperto, potrete rimuovere direttamente i file dal disco virtuale assegnato al vault. Attenersi alla seguente procedura:

1. Aprire Documenti (fare clic su menu Start di Windows e poi **Risorse del computer**).
2. Inserire l'unità disco virtuale corrispondente al vault. Cercare la lettera dell'unità assegnata al vault quando lo si è aperto.
3. Rimuove file o cartelle come si fa normalmente in Windows (ad esempio, fare clic con il pulsante destro su un file che si vuole eliminare e selezionare **Elimina**).

26. Tune-Up

BitDefender è dotato di un modulo di Ottimizzazione che aiuta a mantenere l'integrità del sistema. Gli strumenti di manutenzione offerti sono fondamentali per il miglioramento della reattività del sistema e la gestione efficace dello spazio sul disco rigido.

Per eseguire operazioni di manutenzione sul PC, fare clic su **Ottimizzazione** in Modalità Avanzata ed utilizzare gli strumenti forniti.



Tune-Up

BitDefender fornisce i seguenti strumenti di ottimizzazione del PC:

- Deframmentazione Disco riorganizza fisicamente i dati sul disco rigido in modo che i frammenti di ogni file vengano immagazzinati assieme ed in modo continuo.
- Pulizia PC rimuove i file temporanei di Internet ed i cookie, i file di sistema non utilizzati e i collegamenti a documenti recenti.
- Ricerca Duplicati trova ed elimina i file duplicati sul vostro sistema.
- Pulizia del Registro identifica ed elimina le referenze non aggiornate od invalide dal Registro di Windows. Per mantenere il Registro di Windows pulito ed ottimizzato si consiglia di eseguire la Pulizia del Registro mensilmente.

- Recupero del Registro può ritrovare chiavi di registro cancellate precedentemente dal Registro di Windows usando la Pulizia di Registro di BitDefender.
- Eliminazione definitiva dei File cancella in modo permanente i file e le loro tracce dal vostro sistema.

Per utilizzare uno di questi strumenti, fare clic sul pulsante **Esegui adesso** corrispondente e seguire la procedura guidata.

26.1. Deframmentazione dei Volumi del Disco Rigido.

Quando si copia un file che eccede il blocco più grande di spazio libero su disco rigido, si verifica una frammentazione del file. Siccome non c'è spazio libero sufficiente per immagazzinare l'intero file in modo continuo, verrà immagazzinato in diversi blocchi. Quando si accede al file frammentato, i suoi dati devono essere letti da diverse ubicazioni.

La frammentazione del file rallenta l'accesso allo stesso e diminuisce le prestazioni del sistema. Questo accellera anche l'usura del disco rigido.

Per ridurre la frammentazione dei file dovete deframmentare i dischi periodicamente. La deframmentazione fisica dei dischi riorganizza i dati sul disco rigido in modo che i pezzi di ogni file vengano immagazzinati assieme ed in modo continuo. Questo tenta anche di creare aree di spazio libero più grandi per evitare che i file vengano frammentati dopo.

Si consiglia di deframmentare il disco rigido per:

- accedere più velocemente ai file.
- migliorare le prestazioni del sistema in generale.
- prolungare la vita del disco rigido.

Per deframmentare il disco rigido, seguire questi passaggi:

1. In Modalità Avanzata, fare clic su **Ottimizzazione** nel menu a sinistra.
2. Fare clic sul pulsante **Esegui Adesso** corrispondente al Deframmentazione Disco.
3. Seguire la procedura guidata di tre passaggi. Per ulteriori informazioni fare riferimento a «*Procedura guidata Deframmentazione Disco*» (p. 84).

Nota

La deframmentazione può impiegare un po' di tempo dal momento in cui implica lo spostamento di porzioni di dati immagazzinati da un posto all'altro del disco rigido. Vi consigliamo di eseguire la deframmentazione quando non state usando il vostro computer.

26.2. Pulizia del vostro PC

Ogni volta che visitate una pagina web, vengono creati dei file temporanei Internet per permettervi un accesso più veloce la volta successiva. Nonostante vengono

riferiti come temporanei, questi file non vengono eliminati quando chiudete il browser. Questo può diventare un problema di privacy poichè questi file possono essere visti da chiunque abbia accesso al vostro computer. Inoltre, con il tempo, questi file raggiungono una dimensione considerevole, mangiandosi lo spazio del vostro disco rigido.

Anche i cookies vengono immagazzinati nel vostro computer quando visitate una pagina web. I cookies son dei piccoli file contenenti informazioni sulle vostre preferenze di navigazione. Essi potrebbero essere visti anche come un problema di privacy, poichè possono essere analizzati ed usati dai pubblicisti per tracciare i vostri interessi e gusti on line.

La Pulizia del PC vi aiuta a liberare spazio su disco ed a proteggere la vostra privacy eliminando i file che non vi saranno più utili.

- File temporanei Interrnet e cookie di Internet Explorer.
- File temporanei Interrnet e cookie di Mozilla Firefox.
- file di sistema temporanei creati da Windows durante la sua operazione.
- collegamenti ai documenti recenti creati da Windows quando aprite un file.

Per pulire il sistema da file temporanei Internet e cookie, file di sistema temporanei e collegamenti a documenti recenti, seguire questi passaggi:

1. In Modalità Avanzata, fare clic su **Ottimizzazione** nel menu a sinistra.
2. Fare clic sul pulsante **Esegui adesso** corrispondente alla Pulizia PC.
3. Seguire la procedura guidata di tre passaggi. Per ulteriori informazioni fare riferimento a «*Procedura guidata pulizia PC*» (p. 88).

26.3. Eliminazione Definitiva dei File

Quando eliminate un file, non si può più accedere ad esso con i normali strumenti. Comunque, il file continua ad essere immagazzinato sul disco rigido finchè non verrà sovrascritto quando copierete nuovi file.

Anche se eliminate un file, esso può essere recuperato utilizzando dei programmi specializzati. Questo potrebbe rappresentare una minaccia alla vostra privacy, poichè ci potrebbero essere dei tentativi maligni di prendere i vostri dati privati.

Per evitare che i dati sensibili vengano recuperati dopo che li avete eliminati, potete utilizzare BitDefender per eliminarli definitivamente, rimuovendoli fisicamente dal vostro disco rigido.

Per eliminare definitivamente i file, seguire questi passaggi:

1. In Modalità Avanzata, fare clic su **Ottimizzazione** nel menu a sinistra.
2. Fare clic sul pulsante **Esegui adesso** corrispondente alla Distruzione dei file.

3. Seguire la procedura guidata di tre passaggi. Per ulteriori informazioni fare riferimento a «*Procedura guidata distruzione file*» (p. 102).

26.4. Pulizia del Registro di Windows

Il Registro di Windows è una parte importante dei sistemi operativi Windows. Esso è un database che contiene informazioni ed impostazioni per l'hardware ed il sistema operativo, applicazioni installate, utenti, preferenze del vostro computer ed altro.

Molte applicazioni scrivono delle chiavi nel Registro di Windows al momento dell'installazione. Quando tali applicazioni vengono rimosse, alcune delle chiavi di registro associate potrebbero non venire eliminate e rimanere nel Registro di Windows, rallentando il vostro sistema e causando addirittura instabilità nel sistema. La stessa cosa accade quando eliminate dei collegamenti o certi file di applicazioni installate nel vostro sistema, così come nel caso di driver corrotti.

Per pulire il Registro di Windows e migliorare le prestazioni del vostro sistema, utilizzare lo Strumento di Pulizia del Registro. Lo Strumento di Pulizia esamina il Registro di Windows ed elimina le chiavi di registro non valide.

Per pulire il Registro di Windows, seguire questi passaggi:

1. In Modalità Avanzata, fare clic su **Ottimizzazione** nel menu a sinistra.
2. Fare clic sul pulsante **Esegui adesso** corrispondente alla Pulizia del Registro.
3. Seguire la procedura di quattro passaggi. Per ulteriori informazioni fare riferimento a «*Procedura guidata Pulitore Registro*» (p. 95).

26.5. Recupero di Registro Cancellato

A volte, dopo la pulizia del registro, potreste notare che il vostro sistema non lavora bene, o che alcune applicazioni non operano correttamente, a causa di chiavi di registro mancanti. Questo può essere causato da chiavi di registro condivise che sono state eliminate durante la pulizia del registro o da altre chiavi eliminate. Per risolvere questo problema dovete recuperare il registro pulito.

Per recuperare il registro pulito, seguire questi passaggi:

1. In Modalità Avanzata, fare clic su **Ottimizzazione** nel menu a sinistra.
2. Fare clic sul pulsante **Esegui adesso** corrispondente a Recupero Registro.
3. Seguire la procedura di due passaggi. Per ulteriori informazioni fare riferimento a «*Procedura guidata Ripristino Registro*» (p. 100).

Importante
Solo gli utenti con diritti di amministrazione possono recuperare il registro pulito.

26.6. Trovare file duplicati

I file duplicati si mangiano lo spazio del vostro disco rigido. Pensate solo di avere lo stesso file `.mp3` salvato in tre ubicazioni diverse.

Per rilevare ed eliminare file duplicati dal vostro computer, potete utilizzare il Ricercatore di Duplicati. In questo modo potrete migliorare la gestione dello spazio libero sui vostri dischi rigidi.

Per trovare file duplicati sul vostro computer, seguire questi passaggi:

1. In Modalità Avanzata, fare clic su **Ottimizzazione** nel menu a sinistra.
2. Fare clic sul pulsante **Esegui adesso** corrispondente a Ricercatore file duplicati.
3. Seguire la procedura di quattro passaggi. Per ulteriori informazioni fare riferimento a «*Procedura guidata Ricercatore di Duplicati* » (p. 91).

27. Modalità Gioco / Portatile

La Modalità Gioco / Portatile vi permette di configurare le modalità speciali di operatività di BitDefender:

- Modalità Gioco modifica temporaneamente le impostazioni del prodotto in modo di minimizzare il consumo di risorse mentre giocate.
- Modalità Portatile impedisce che le funzioni programmate vengano eseguite quando il portatile funziona con la batteria in modo da risparmiare energia della batteria.

27.1. Modalità giochi

La Modalità Gioco modifica temporaneamente le impostazioni di protezione in modo di minimizzare l'impatto sulle prestazioni del sistema. Mentre siete in Modalità Gioco, verranno applicate le seguenti impostazioni:

- Tutti gli allarmi e pop-up BitDefender sono disabilitati.
- Il livello di protezione in tempo reale di BitDefender è impostato come **Permissivo**.
- Il Firewall BitDefender è impostato con **Consentire tutti**. Questo significa che tutte le nuove connessioni (sia in entrata che in uscita) vengono consentite, indipendentemente della porta o protocollo utilizzati.
- Gli aggiornamenti non vengono eseguiti di default.

Nota

Per cambiare queste impostazioni, cliccare su Aggiornamento > Impostazioni e deselezionare la casella **Non aggiornare se la Modalità Gioco è attiva**.

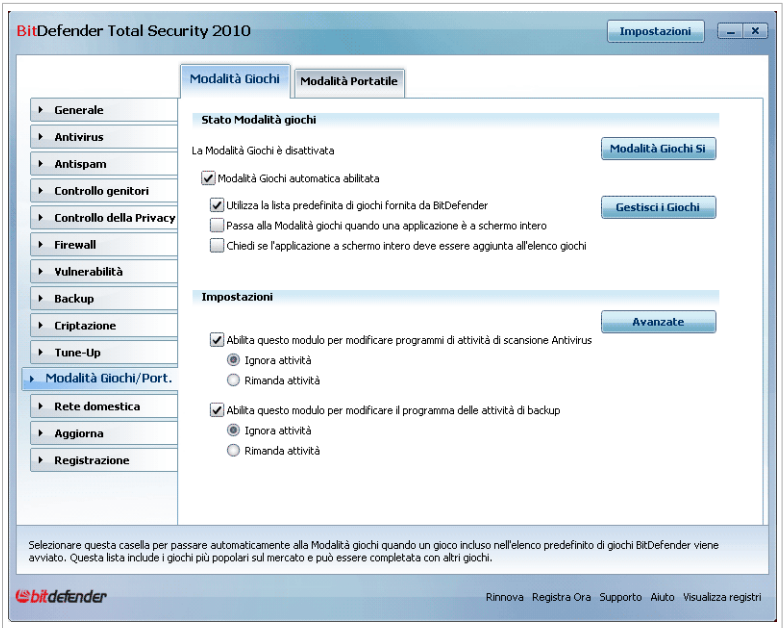
- Le funzioni di scansione programmate sono disabilitate di default.
- Le funzioni programmate di backup sono disabilitate di default.

Di default, BitDefender entra automaticamente in Modalità Gioco quando iniziate un gioco incluso nella lista BitDefender dei giochi conosciuti o quando un'applicazione passa a schermo pieno. Potete entrare manualmente in Modalità Gioco usando la hotkey di default `Ctrl+Alt+Shift+G`. E' fortemente consigliato di uscire dalla Modalità Gioco quando avete finito di giocare (potete usare la stessa hotkey di default `Ctrl+Alt+Shift+G`).

Nota

Mentre siete in Modalità Gioco, potete vedere la lettera G sull' icona BitDefender.

Per configurare la Modalità Gioco, andare su **Modalità Gioco / Laptop>Modalità Gioco** in Modalità Avanzata.


BitDefender Total Security 2010
Impostazioni
Modalità Giochi
Modalità Portatile
Generale
Antivirus
Antispam
Controllo genitori
Controllo della Privacy
Firewall
Vulnerabilità
Backup
Criptazione
Tune-Up
Modalità Giochi/Port.
Rete domestica
Aggiorna
Registrazione
Stato Modalità giochi
La Modalità Giochi è disattivata
Modalità Giochi Si
Modalità Giochi automatica abilitata
Utilizza la lista predefinita di giochi fornita da BitDefender
Passa alla Modalità giochi quando una applicazione è a schermo intero
Chiedi se l'applicazione a schermo intero deve essere aggiunta all'elenco giochi
Gestisci i Giochi
Impostazioni
Avanzate
Abilita questo modulo per modificare programmi di attività di scansione Antivirus
Ignora attività
Rimanda attività
Abilita questo modulo per modificare il programma delle attività di backup
Ignora attività
Rimanda attività
Selezionare questa casella per passare automaticamente alla Modalità giochi quando un gioco incluso nell'elenco predefinito di giochi BitDefender viene avviato. Questa lista include i giochi più popolari sul mercato e può essere completata con altri giochi.
bitdefender
Rinnova Registra Ora Supporto Aiuto Visualizza registri

Modalità giochi

Nella parte superiore della sezione è possibile vedere lo stato della Modalità Gioco. È possibile fare clic su **Attiva Modalità giochi** o **Disattiva Modalità giochi** per cambiare lo stato attuale.

27.1.1. Configurazione Automatica della Modalità Gioco

La Modalità Gioco automatica consente a BitDefender di entrare in Modalità Gioco quando un gioco viene rilevato. E' possibile configurare le seguenti opzioni:

- **Usare la lista di default dei giochi fornita da BitDefender** - per entrare automaticamente in Modalità Gioco quando iniziate un gioco della lista dei giochi conosciuti da BitDefender. Per vedere questo elenco, fare clic su **Gestione giochi** e quindi su **Elenco giochi**.
- **Entrare nella Modalità giochi quando una applicazione è a schermo pieno** - per entrare automaticamente nella Modalità giochi quando un'applicazione passa a schermo pieno.
- **Aggiungere l'applicazione alla lista dei giochi?** - perchè vi venga richiesto di aggiungere una nuova applicazione alla lista dei giochi quando abbandonate lo schermo pieno. Aggiungendo una nuova applicazione alla lista dei giochi, la

prossima volta che la avvierete BitDefender entrerà automaticamente in Modalità Gioco.

Nota
Se non desiderate che BitDefender entri automaticamente in Modalità Gioco, deselezionare la casella **Modalità Gioco Automatica**.

27.1.2. Gestione della Lista dei Giochi

BitDefender entra automaticamente in Modalità Gioco quando avviate una applicazione dalla lista dei giochi. Per visualizzare e gestire la lista dei giochi, cliccare su **Gestire Giochi**. Apparirà una nuova finestra.

Gestisci giochi BitDefender
Elenco Miei Giochi
Nome
Elenco giochi
Questo è l'elenco di giochi che causeranno a BitDefender di avviare automaticamente la Modalità giochi.
OK

Lista dei Giochi

Nuove applicazioni vengono automaticamente aggiunte alla lista quando:

- Avviate un gioco dalla lista dei giochi conosciuti di BitDefender. Per visualizzare la lista, fare clic su **Elenco giochi**.
- Dopo aver abbandonato lo schermo pieno, aggiungete l'applicazione alla lista dei giochi dalla finesta proposta.

Se volete disabilitare la Modalità Gioco Automatica per un'applicazione specifica della lista, deselezionare la casella corrispondente. Dovreste disabilitare la Modalità Gioco Automatica per le applicazioni regolari che vanno in schermo pieno, come web browser o movie player.

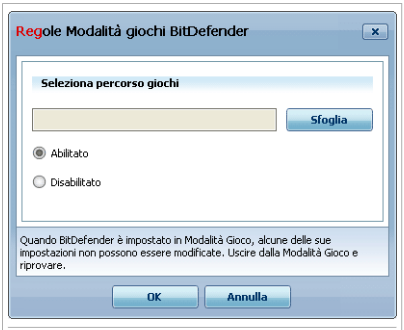
Per gestire questa lista giochi, potete usare i tasti situati nella parte superiore della tabella:

- Cliccare su **OK** per aggiungere la nuova applicazione alla lista dei giochi.

- **Rimuovi** - per rimuovere tutte le applicazioni installate.
- Cliccare su **OK** per aggiungere l'applicazione alla lista dei giochi.

Aggiungere o Modificare Giochi

Quando aggiungete o modificate un'entrata della lista dei giochi, apparirà la seguente finestra:


Regole Modalità giochi BitDefender
Seleziona percorso giochi
Sfoglia
Abilitato
Disabilitato
Quando BitDefender è impostato in Modalità Gioco, alcune delle sue impostazioni non possono essere modificate. Uscire dalla Modalità Gioco e riprovare.
OK
Annulla

Aggiungere Gioco

Cliccare su **Sfoglia** per selezionare l'applicazione o digitare il percorso completo dell'applicazione nel campo corrispondente.

Se non si desidera entrare automaticamente in Modalità Gioco quando l'applicazione è già iniziata, selezionare **Disabilitare**.

Cliccare su **OK** per aggiungere l'entrata alla lista dei giochi.

27.1.3. Configurazione delle Impostazioni della Modalità Gioco

Per configurare il comportamento delle funzioni programmate, usare queste opzioni:

- **Abilitare questo modulo per modificare le programmazioni attività scansione antivirus** - per impedire che attività di scansione programmate vengano eseguite mentre si è nella Modalità giochi. E' possibile selezionare una delle seguenti opzioni:

Opzione	Descrizione
Saltare Task	Non eseguire la funzione programmata.
Posporre Task	Eseguire la funzione programmata immediatamente dopo che siete usciti dalla Modalità Gioco.

- **Abilitare questo modulo per modificare le programmazioni attività di backup** - per impedire che attività di backup programmate vengano eseguite mentre si è nella Modalità giochi. E' possibile selezionare una delle seguenti opzioni:

Opzione	Descrizione
Saltare Task	Non eseguire la funzione programmata.
Posporre Task	Eseguire la funzione programmata immediatamente dopo che siete usciti dalla Modalità Gioco.

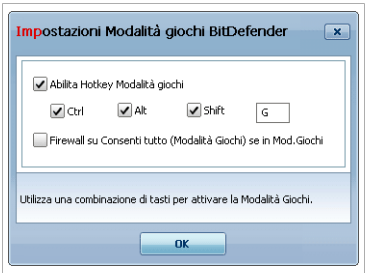
Per disabilitare automaticamente il Firewall BitDefendere quando vi troviate in Modalità Gioco, seguire questi passaggi:

1. Cliccare su **Impostazioni Avanzate**. Apparirà una nuova finestra.
2. Selezionare la casella di controllo **Imposta Firewall su Consenti tutto (Modalità giochi) quando in Modalità giochi**.
3. Selezionare **Applica** per salvare le modifiche.

27.1.4. Modifica Hotkey della Modalità Gioco.

Potete entrare manualmente in Modalità Gioco usando la hotkey di default `Ctrl+Alt+Shift+G`. Per modificare la hotkey, seguire questi passaggi:

1. Cliccare su **Impostazioni Avanzate**. Apparirà una nuova finestra.



Avanzate

2. Sotto l'opzione **Usare HotKey**, impostare la hotkey desiderata:
   - Scegliere i tasti di modifica che si vogliono usare selezionando uno dei seguenti: tasto Control (`Ctrl`), tasto Maiuscola (`Shift`) o tasto Alternare (`Alt`).
   - Nel campo editabile, inserire la lettera corrispondente al tasto regolare che si vuole usare.

Ad esempio, se volete usare la hotkey `Ctrl+Alt+D`, dovete solo controllare i tasti `Ctrl` e `Alt` ed inserire la `D`.

Nota
Deselezionare la casella **Usare HotKey** disabiliterà la hotkey.

3. Selezionare **Applica** per salvare le modifiche.

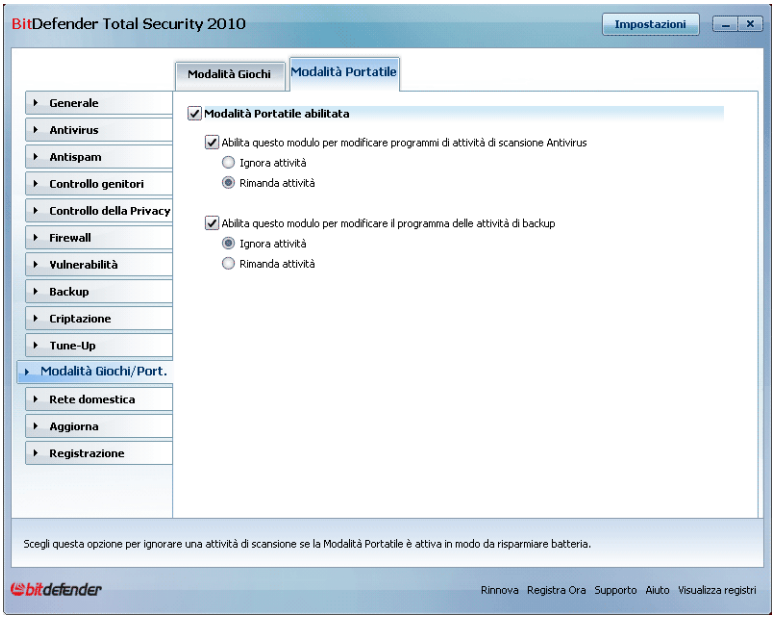
27.2. Modalità Portatile

La Modalità Portatile è stata specialmente disegnata per chi usa i laptop/notebook. Il suo proposito è minimizzare l'impatto di BitDefender sul consumo di energia mentre questi apparecchi funzionino con la batteria.

Mentre siete in Modalità Portatile, le funzioni programmate non verranno eseguite di default.

BitDefender rileva quando il vostro portatile sta funzionando con la batteria ed automaticamente va in Modalità Portatile. Nello stesso modo, BitDefender uscirà automaticamente dalla Modalità Portatile quando rileverà che il portatile non sta più lavorando con la batteria.

Per configurare la Modalità Portatile, andare su **Modalità Gioco / Portatile>Modalità Portatile** in Modalità Avanzata.



Modalità Portatile

Potete vedere se la Modalità Portatile è abilitata o meno. Se la Modalità Portatile è abilitata, BitDefender applicherà le impostazioni configurate mentre il portatile lavora con la batteria.

27.2.1. Configurazione delle Impostazioni della Modalità Portatile

Per configurare il comportamento delle funzioni programmate, usare queste opzioni:

- **Abilitare questo modulo per modificare le programmazioni attività scansione antivirus** - per impedire che attività di scansione programmate vengano eseguite mentre si è nella Modalità portatile. E' possibile selezionare una delle seguenti opzioni:

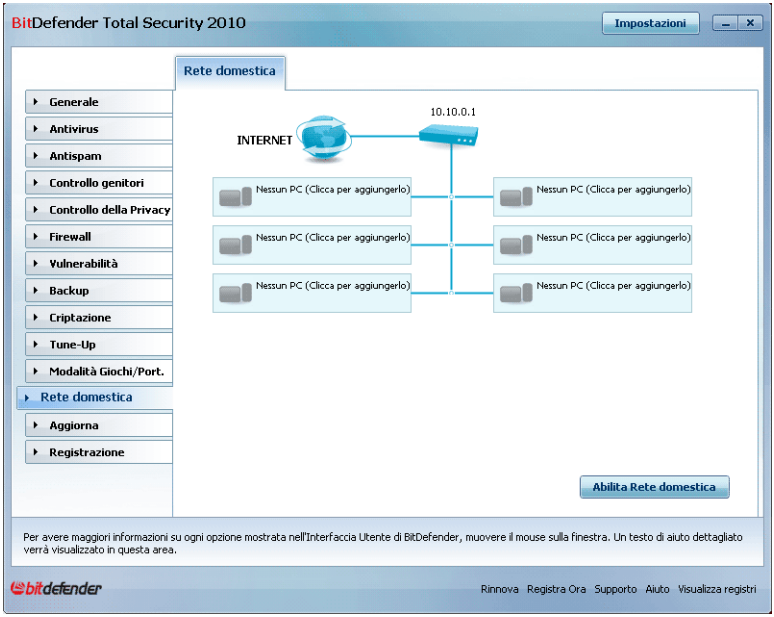
Opzione	Descrizione
Saltare Task	Non eseguire la funzione programmata.
Posporre Task	Eseguire la funzione programmata immediatamente dopo che siete usciti dalla Modalità Portatile.

- **Abilitare questo modulo per modificare le programmazioni attività di backup** - per impedire che attività di backup programmate vengano eseguite mentre si è nella Modalità portatile. E' possibile selezionare una delle seguenti opzioni:

Opzione	Descrizione
Saltare Task	Non eseguire la funzione programmata.
Posporre Task	Eseguire la funzione programmata immediatamente dopo che siete usciti dalla Modalità Portatile.

28. Rete domestica

Il modulo Rete vi permette gestire i prodotti BitDefender installati sui computer di casa da un singolo computer.



Mappa di rete

Per essere in grado di gestire i prodotti BitDefender installati sui computer di casa, dovete seguire questi passaggi:

1. Unirvi alla rete domestica BitDefender sul vostro computer. Unirsi alla rete consiste in configurare una password di amministrazione per la gestione della rete domestica.
2. Andare su ogni computer che si vuole gestire ed aggiungerli alla rete (impostare la password).
3. Tornare al vostro computer ed aggiungere i computer che volete gestire.

28.1. Unirsi alla Rete BitDefender

Per unirsi alla rete domestica BitDefender, seguire questi passaggi:

1. Fare clic su **Abilita rete**. Vi verrà chiesto di configurare le password per la gestione domestica.

BitDefender
Digitare password rete domestica
E' richiesta una password per accedere o creare una rete per motivi di sicurezza.Questa password proteggerà l'accesso al computer attraverso la rete domestica.
Password:
Reinserisci password:
OK
Annulla

Configurare Password

2. Inserire la stessa password in ognuno dei campi corrispondenti.
3. Selezionare **OK**.

Potete vedere il nome del computer apparire nella mappa della rete.

28.2. Aggiungere dei computer alla Rete BitDefender

Prima di poter aggiungere un computer alla rete domestica BitDefender dovrete configurare la password per la gestione domestica BitDefender sul rispettivo computer.

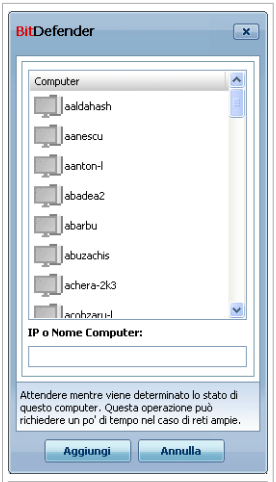
Per aggiungere un computer alla rete domestica BitDefender , seguire questi passi:

1. Fare clic su **Aggiungi Computer**. Vi verrà chiesto di fornire la password per la gestione domestica locale.

BitDefender
Inserire qui la password impostata quando è stata abilitata la Gestione domestica su questo PC.
Password
Non mostrare più questo messaggio durante questa sessione.
OK
Annulla

Inserire Password

2. Digitare la password per la gestione domestica e cliccare su **OK**. Apparirà una nuova finestra.

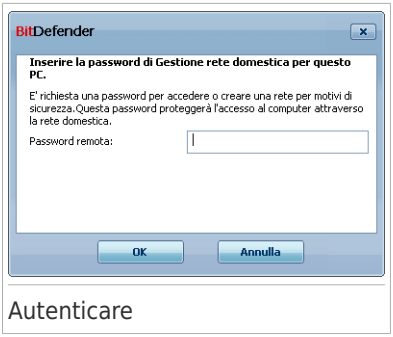


Aggiungi Computer

Potete vedere l'elenco dei computer in questa rete. Il significato dell'icona è il seguente:

- Indica un computer online senza prodotti BitDefender installati.
- Indica un computer online con BitDefender installato.
- Indica un computer offline con BitDefender installato.

3. Eseguire una delle seguenti azioni:
   - Selezionare dall'elenco il nome del computer da aggiungere.
   - Digitare l'indirizzo IP o il nome del computer da aggiungere nel campo corrispondente.
4. Selezionare **Aggiungi**. Vi verrà chiesto di fornire la password per la gestione domestica sul rispettivo computer.


BitDefender
Inserire la password di Gestione rete domestica per questo PC.
E' richiesta una password per accedere o creare una rete per motivi di sicurezza. Questa password proteggerà l'accesso al computer attraverso la rete domestica.
Password remota:
OK
Annulla

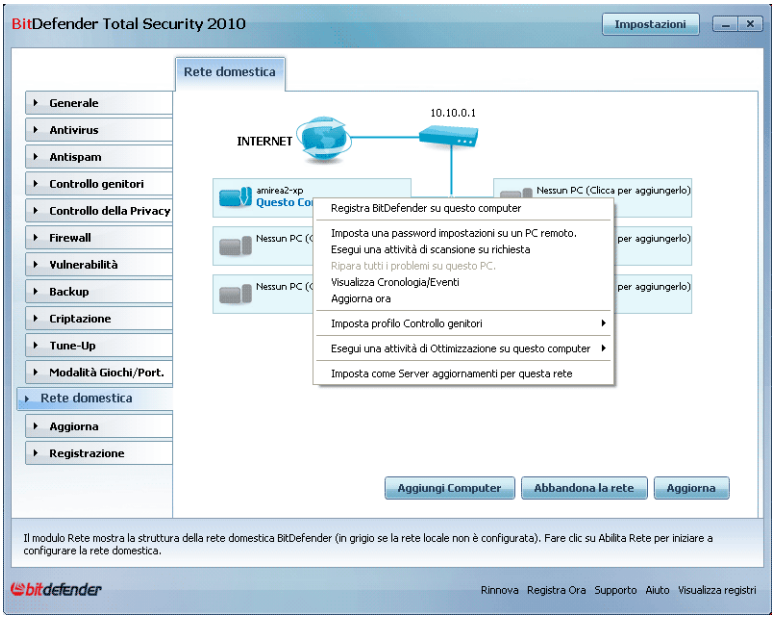
Autenticare

5. Digitare la password per la gestione domestica configurata sul rispettivo computer.
6. Selezionare **OK**. Se avete fornito la password corretta, il nome del computer selezionato apparirà nella mappa di rete.

Nota
Potete aggiungere fino a cinque computer alla mappa di rete.

28.3. Gestione della Rete BitDefender

Una volta che avete creato con successo una rete domestica BitDefender, potrete gestire tutti i prodotti BitDefender da un singolo computer.



Mappa di rete

Se muovete il cursore su un computer nella mappa di rete, potete vedere una breve informazione su di esso (nome, indirizzo IP, numero di problemi che colpiscono la sicureza del sistema, stato della registrazione di BitDefender).

Se si fa clic sul nome di un computer nella mappa di rete, è possibile vedere tutte le funzioni di amministrazione che si possono eseguire sul computer remoto.

- **Rimuovi il PC dalla rete domestica**

  Permette di rimuovere il PC dalla rete.

- **Registra BitDefender su questo computer**

  Permette di registrare BitDefender sul computer inserendo una chiave di licenza.

- **Stabilire una password per le impostazioni su un PC remoto**

  Permette di creare una password per limitare l'accesso alle impostazioni BitDefender sul PC.

- **Eseguire una attività di scansione su richiesta**

  Permette di eseguire una scansione a richiesta sul computer remoto. E' possibile compiere una qualsiasi delle seguenti attività di scansione: Scansione Documenti, Scansione del Sistema o Scansione del Sistema Approfondita.

- **Risolvere tutti i problemi su questo computer**

  Permette di risolvere i problemi che influenzano la sicurezza del computer seguendo l'assistente Risolvi Tutti i Problemi.

- **Visualizzare Cronologia/Eventi**

  Permette di accedere al modulo **Cronologia&Eventi** del prodotto BitDefender installato sul computer.

- **Aggiorna adesso**

  Avvia il processo di aggiornamento per il prodotto BitDefender installato sul computer.

- **Imposta Profilo Controllo genitori**

  Permette di impostare la categoria di età da utilizzare per il filtro web del Controllo Genitori del computer: bambino, adolescente o adulto.

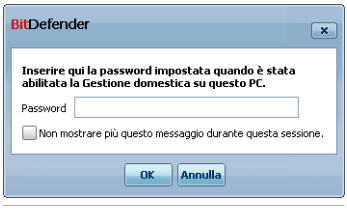
- **Esegui una funzione di Ottimizzazione su questo computer**

  Permette di eseguire un'attività di ottimizzazione sul PC remoto. E' possibile eseguire una delle seguenti attività: deframmentazione dischi o pulizia dei file temporanei di Internet.

- **Impostare come Server di aggiornamento per questa rete**

  Permette di impostare il computer come server di aggiornamento per tutti i prodotti BitDefender installati sui computer della rete. Utilizzando questa opzione si ridurrà il traffico Internet, poiché un solo computer della rete si collegherà ad Internet per scaricare gli aggiornamenti.

Prima di eseguire una funzione su un particolare computer, vi verrà chiesto di fornire la password per la gestione domestica locale.


BitDefender
Inserire qui la password impostata quando è stata abilitata la Gestione domestica su questo PC.
Password
Non mostrare più questo messaggio durante questa sessione.
OK
Annulla

Inserire Password

Digitare la password per la gestione domestica e cliccare su **OK**.

Nota

Se programmate di eseguire più funzioni, potete selezionare **Non mostrare di nuovo questo messaggio durante questa sessione**. Selezionando questa opzione non vi verrà più chiesta la password durante la sessione corrente.

29. Aggiorna

Tutti giorni vengono trovati ed identificati nuovi malware. E' quindi molto importante mantenere aggiornato il vostro BitDefender con le impronte più recenti del malware.

Se siete connessi ad Internet con banda larga o DSL, BitDefender si prenderà cura di sè da solo. Per default, esso cercherà degli aggiornamenti, ogni volta che avvierete il vostro computer ed ogni **ora**dopo l'avvio.

Se viene rilevato un aggiornamento, vi verrà chiesto di confermare l'aggiornamento o l'aggiornamento verrà eseguito automaticamente, a seconda delle impostazioni dell'aggiornamento automatico update settings.

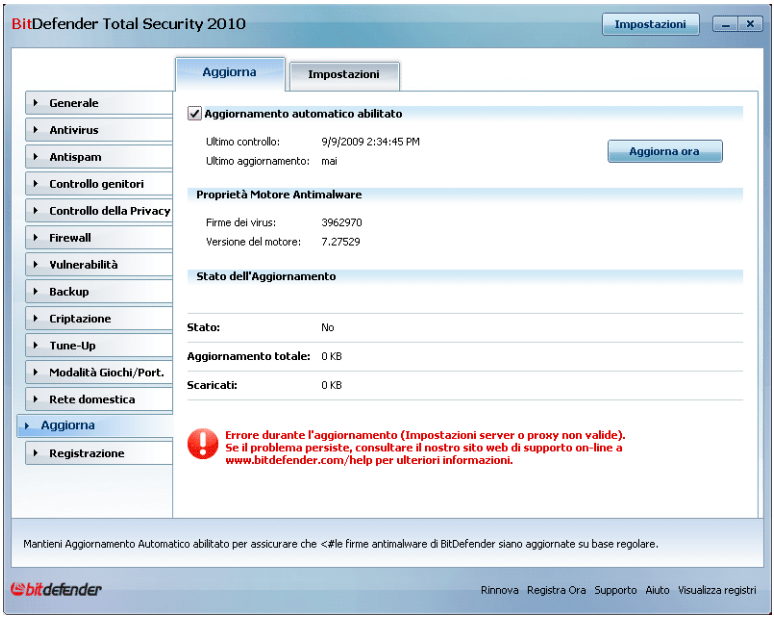
Il processo di aggiornamento viene eseguito involo, il chè vuol dire che i file da aggiornare vengono sostituiti progressivamente. In questo modo, il processo di aggiornamento non interesserà l'operatività del prodotto, nello stesso tempo, ogni vulnerabilità verrà esclusa.

Gli Aggiornamenti arrivano nei seguenti modi:

- **Aggiornamenti per motori Antivirus** - non appena compaiono nuove minacce, i file contenenti le impronte dei virus devono essere aggiornati per garantire una protezione aggiornata permanente contro queste nuove minacce. Questo tipo di aggiornamento è anche conosciuto come **Virus Definitions Update**.
- **Aggiornamenti per motori Antispam** - verranno aggiunte nuove regole ai filtri euristico ed URL, e nuove immagini al filtro immagini. Ciò contribuirà ad aumentare l'efficacia del vostro motore Antispam. Questo tipo di aggiornamento è anche conosciuto come **Antispam Update**.
- **Aggiornamento per I motori antispyware** - nuove firme antispyware saranno aggiunte al database. Questo tipo di aggiornamento è anche conosciuto come **Antispyware Update**.
- **Aggiornamenti del Prodotto** - quando viene rilasciata la nuova versione di un prodotto, vengono introdotte nuove funzionalità e tecniche di scansione al fine di migliorare l'efficienza del prodotto. Questo tipo di aggiornamento è anche conosciuto come **Product Update**.

29.1. Aggiornamento Automatico

Per visualizzare informazioni relative all'aggiornamento ed eseguire aggiornamenti automatici, fare clic su **Aggiornamento>Aggiornamento** in Modalità Avanzata.



Aggiornamento Automatico

Qui è possibile visualizzare quando sono stati eseguiti l'ultimo controllo degli aggiornamenti e l'ultimo aggiornamento, così come le informazioni sull'ultimo aggiornamento eseguito (se con successo o gli errori verificatisi). Inoltre si mostrano informazioni sulla versione del motore corrente ed il numero di impronte.

se aprite questa sezione durante un aggiornamento potrete visualizzare lo stato del download.

Importante
Per essere sempre protetti, tenete l' **Aggiornamento Automatico** abilitato.

29.1.1. Richiedere un aggiornamento

L'aggiornamento automatico può essere eseguito in qualsiasi momento, cliccando su **Aggiornare adesso**. Questo aggiornamento è conosciuto anche come **Aggiornamento su richiesta dell'utente**.

Il modulo **Aggiornamento** si collegherà al server di aggiornamento di BitDefender e verificherà la disponibilità. Se viene rilevato un aggiornamento, secondo le opzioni impostate nella sezione Impostazioni Aggiornamento Manuale, vi verrà chiesto di confermarlo oppure verrà eseguito automaticamente.

Importante
Può essere necessario riavviare il computer una volta completato l'aggiornamento. Noi consigliamo di farlo al più presto possibile.

Nota
Se siete connessi a Internet mediante una connessione telefonica, è consigliato l'aggiornamento periodico di BitDefender su richiesta dell'utente.

29.1.2. Disattivare Aggiornamento Automatico

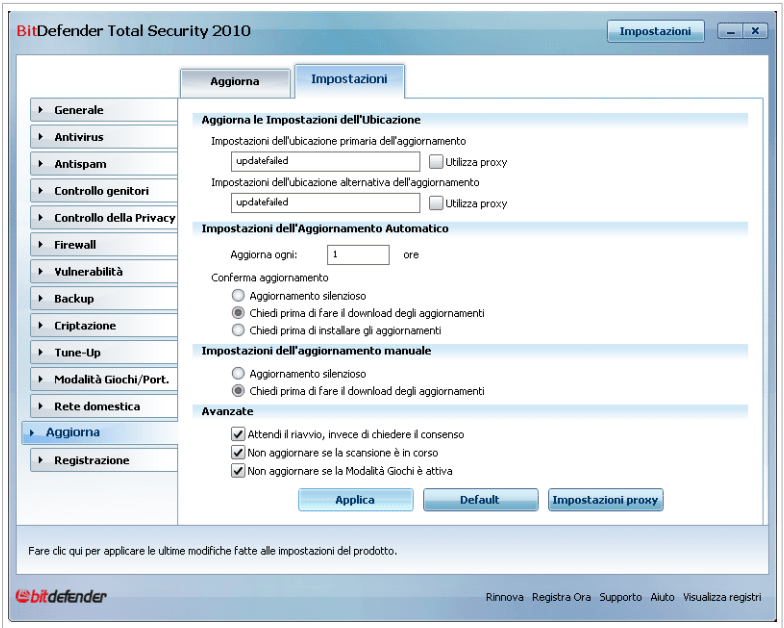
Scegliendo di disattivare l'aggiornamento automatico, apparirà una finestra di avviso. Dovete confermare la vostra scelta selezionando dal menu per quanto tempo volete che l'aggiornamentop automatico venga disattivato. Potete disattivare l'aggiornamento automatico per 5, 15 o 30 minuti, per un'ora, permanentemente o fino al riavvio del sistema.

Avvertimento
Questa è una questione critica di sicurezza. Vi consigliamo di disattivare l'aggiornamento automatico per il minimo tempo possibile. Se BitDefender non verrà aggiornato regolarmente non sarà in grado di proteggervi dalle minacce più recenti.

29.2. Impostazioni dell'aggiornamento

Gli aggiornamenti possono essere eseguiti dalla rete locale, su Internet, direttamente o attraverso un server proxy. Per default, BitDefender controllerà la disponibilità di aggiornamenti ogni ora sulla Internet ed installerà gli aggiornamenti disponibili senza avvisarvi.

Per configurare le impostazioni di aggiornamento e gestire i proxy, fare clic su **Aggiornamento>Impostazioni** in Modalità Avanzata.



Impostazioni dell'aggiornamento

Le impostazioni dell'aggiornamento sono ragruppate in 4 categorie (**Impostazioni Ubicazione Aggiornamento**, **Impostazioni Aggiornamento Automatico**, **Impostazioni Aggiornamento Manuale** ed **Impostazioni Avanzate**). Ogni categoria verrà descritta separatamente.

29.2.1. Impostare Ubicazioni Aggiornamento

Per configurare le ubicazioni dell'aggiornamento utilizzare le opzioni della categoria **Impostazioni Ubicazione Aggiornamento**.

Nota

Configurare queste impostazioni solo se siete connessi ad una rete locale che immagazzini localmente le impronte malware di BitDefender o se vi connettete ad Internet attraverso un server proxy.

Per aggiornamenti più affidabili e veloci, potete configurare due ubicazioni per l'aggiornamento: **Ubicazione principale dell'aggiornamento** e **Ubicazione alternativa dell'aggiornamento**. Di default, queste ubicazioni sono la stessa:`http://upgrade.bitdefender.com`.

Per modificare una delle ubicazioni dell'aggiornamento, inserire l'URL dello specchio locale nel campo **URL** corrispondente all'ubicazione che si desidera modificare.

Nota
Vi consigliamo di impostare come ubicazione principale dell'aggiornamento lo specchio locale e di non modificare l'ubicazione alternativa, come piano di sicurezza interna nel caso in cui lo specchio locale non fosse disponibile.

Nel caso in cui l'azienda usi un server proxy per connettersi ad internet, selezionare **Usa proxy** e poi fare clic su **Impostazioni proxy** per configurare le impostazioni proxy. Per ulteriori informazioni, vi preghiamo di riferirvi a *«Gestione Proxies»* (p. 344)

29.2.2. Configurazione Aggiornamento Automatico

Per configurare l'esecuzione automatica del processo di aggiornamento da parte di BitDefender, utilizzare le opzioni della categoria **Impostazioni Aggiornamento Automatico**.

È possibile specificare il numero di ore tra due controlli consecutivi per aggiornamenti nel campo **Aggiorna ogni**. Per default l'intervallo di tempo tra aggiornamenti è impostato ad un'ora.

Per specificare come dovrebbe essere eseguito il processo di aggiornamento automatico, selezionare una delle seguenti opzioni:

- **Aggiornamento silenzioso** - BitDefender scarica ed implementa l'aggiornamento automaticamente.
- **Chiedere prima di scaricare gli aggiornamenti** - ogni volta che un aggiornamento è disponibile, vi verrà richiesto se eseguire il download.
- **Chiedere prima di installare gli aggiornamenti** - ogni volta che si scarica un aggiornamento, vi verrà richiesto se installarlo.

29.2.3. Configurazione Aggiornamento Manuale

Per specificare come dovrà essere eseguito l'aggiornamento manuale (aggiornamento a richiesta dell'utente) selezionare una delle seguenti opzioni dalla categoria **Impostazioni Aggiornamento Manuali**:

- **Aggiornamento silenzioso** - l'aggiornamento manuale verrà eseguito automaticamente in background, senza l'intervento dell'utente.
- **Chiedere prima di scaricare gli aggiornamenti** - ogni volta che un aggiornamento è disponibile, vi verrà richiesto se eseguire il download.

29.2.4. Configurazione delle Impostazioni Avanzate

Per evitare che il processo di aggiornamento di BitDefender interferisca con il vostro lavoro, configurare le opzioni nella categoria **Impostazioni Avanzate**:

- **Attendi conferma prima di riavviare** - Se un aggiornamento richiede un riavvio, il prodotto continuerà a lavorare con i vecchi file finche il sistema venga riavviato. Non verrà chiesto all'utente di riavviare, a fin che il processo di aggiornamento non interferisca con il lavoro dell'utente.
- **Non aggiornare se la scansione è attiva** - BitDefender non verrà aggiornato se è in corso un processo di scansione. In tal modo la procedura di aggiornamento BitDefender non interferisce con le operazioni di scansione.

  Nota
  Se BitDefender è aggiornato durante una scansione, la procedura di scansione viene interrotta.

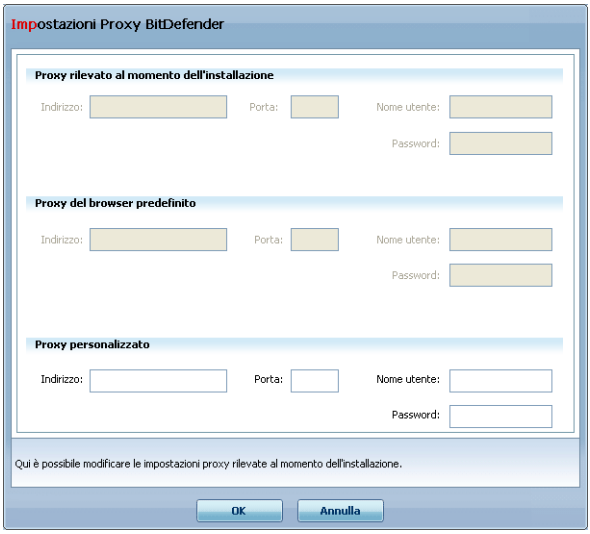
- **Non aggiornare se la modalità gioco è attiva** - BitDefender non eseguirà l'aggiornamento se la modalità gioco è attiva. In questo modo si può minimizzare l'influenza del prodotto sulla performance del vostro sistema durante i giochi.

29.2.5. Gestione Proxies

Se la vostra azienda utilizza un server proxy per connettersi ad Internet, dovrete specificare le impostazioni di proxy perchè BitDefender si possa aggiornare da solo. Altrimenti, esso utilizzerà le impostazioni proxy dell'amministratore che installò il prodotto o, se ci sono, le impostazioni predefinite del browser dell'utente corrente.

Nota
Le impostazioni del proxy possono essere configurate solo da utenti con diritti di amministratore sul computer oppure da "power users" (utenti che conoscono la password per le impostazioni del prodotto).

Per gestire le impostazioni proxy, fare clic su **Impostazioni Proxy**. Apparirà una nuova finestra.



Gestore del proxy

Vi sono tre gruppi di impostazioni del proxy:

- **Proxy rilevato al momento dell'installazione)** - impostazioni del proxy rilevate sull'account dell'amministratore durante l'installazione le quali possono essere configurate solo utilizzando tale account. Se il server proxy richiede un nome utente ed una password, specificarli nei rispettivi campi.
- **Proxy del browser predefinito** - impostazioni proxy dell'utente attuale, tratte dal browser predefinito. Se il server proxy richiede un nome utente e una password, è necessario specificarle nei campi corrispondenti.

  Nota
  I browser web supportati sono Internet Explorer, Mozilla Firefox ed Opera. Se usate un altro browser di default, BitDefender non sarà in grado di ottenere le impostazioni del proxy dell'utente corrente.

- **Proxy personalizzato** - impostazioni del proxy che si possono configurare se si accede come amministratore.

  Le seguenti impostazioni devono essere specificate:
  - **Indirizzo** - inserire l'IP del server proxy.
  - **Porta** - inserire la porta che utilizza BitDefender per connettersi al server proxy.
  - **Nome Utente** - inserire un nome utente riconosciuto dal proxy.
  - **Password** - inserire la password valida per l'utenza, già specificata precedentemente.

Quando ci si tenta di connettere ad Internet, ogni set di impostazione del proxy viene tentato uno alla volta, finchè BitDefender non riesce a connettersi.

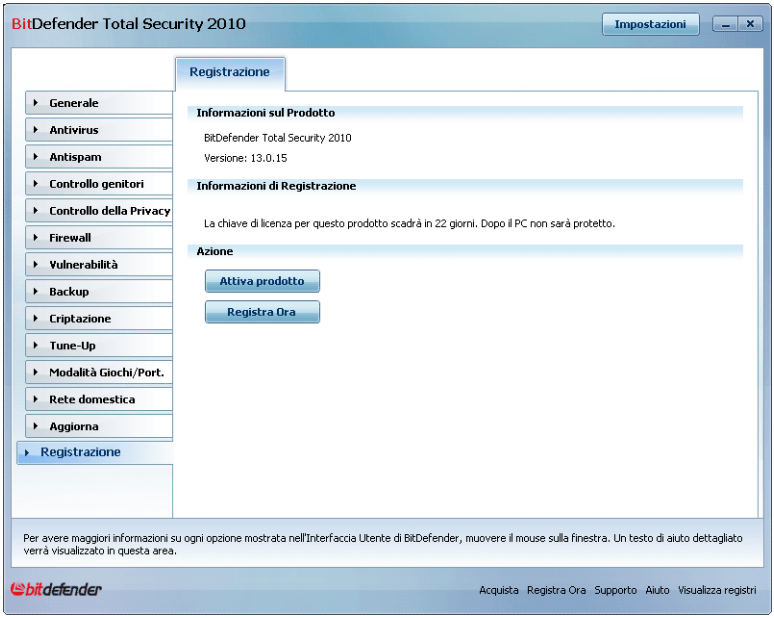
In primo luogo verrà usato il set contenente le vostre impostazioni per connettersi ad Internet. Se questo non funzionasse, verranno utilizzate successivamente le impostazioni del proxy rilevate al momento dell'installazione. Ed infine, se neanche queste funzionassero, le impostazioni del proxy dell'utente corrente verranno ricavate dal browser predefinito ed utilizzate per connettersi ad Internet.

Selezionare **OK** per salvare le modifiche e chiudere la finestra.

Selezionare **Applica** per salvare le modifiche oppure selezionare **Preimpostazione** per tornare alle impostazioni di default.

30. Registrazione

Per trovare informazioni complete sul vostro prodotto BitDefender e sullo stato della registrazione, fare clic su **Registrazione** in Modalità Avanzata.



Registrazione

Questa sezione mostra:

- **Informazioni sul Prodotto**: il prodotto BitDefender e la versione.
- **Informazioni sulla Registrazione**: l'indirizzo mail usato per registrare il vostro account BitDefender (se configurato), la chiave di licenza attuale e quanti giorni mancano fino alla scadenza della licenza.

30.1. Registrazione Sicurezza totale BitDefender 2010

Fare clic su **Registra Ora** per aprire la finestra di registrazione del prodotto.

BitDefender Total Security 2010
Procedura guidata di Registrazione
Registrazione BitDefender
Informazioni chiave di licenza attuale
Tipo: VALIDA, Utente finale
Scade tra: 350 giorni
Codice di licenza: BE089489D2B83E26D4EA
Inserire una chiave di licenza:
Codice di licenza:
Inserire una chiave di licenza
Registra Ora
Non disponi di una chiave di licenza? Acquistane una ora!
Per avere maggiori informazioni su ogni opzione mostrata nell'Interfaccia Utente di BitDefender, muovere il mouse sulla finestra. Un testo di aiuto dettagliato verrà visualizzato in questa area.
Annulla
Indietro
Termina

Registrazione

Potete vedere lo stato della registrazione BitDefender, la chiave di licenza corrente ed i giorni mancanti alla scadenza della licenza.

Per registrare Sicurezza totale BitDefender 2010>

1. Inserire la chiave di licenza nel campo di modifica.

Nota

Potete trovare la vostra chiave di licenza:

- sull'etichetta del CD.
- sulla scheda di registrazione del prodotto.
- sulla mail di acquisto online.

Se non si ha una chiave di licenza BitDefender, fare clic sul link fornito per andare al negozio on-line di BitDefender ed acquistare una.

2. Fare clic su **Registra Ora**.
3. Selezionare **Termina**.

30.2. Creazione di un Account BitDefender

Come parte del processo di registrazione, è necessario creare un account BitDefender L'account BitDefender ti da accesso a supporto tecnico gratis ed a offerte speciali e promozioni. Se avete perso la vostra chiave di licenza BitDefender, potete logarvi sul vostro conto in http://myaccount.bitdefender.com per recuperarla.

Importante

E' necessario creare un account entro 15 giorni dall'installazione di BitDefender (se il prodotto viene registrato con una chiave di licenza, la scadenza è estesa a 30 giorni). Altrimenti, BitDefender non sarà più aggiornato.

Se non si è ancora creato un account BitDefender, fare clic su **Attiva Prodotto** per aprire la finestra di registrazione del prodotto.

BitDefender Total Security 2010
Procedura guidata di Registrazione
Account BitDefender:
Per gli aggiornamenti e l'assistenza,attivare BitDefender creando l'account. L'attivazione può essere rimandata di 15 gg per le versioni di prova e di 30 gg per quelle registrate. Più informazioni su http://www.bitdefender.com/why_register.
Crea un nuovo account
Indirizzo e-mail:
Inserire indirizzo e-mail
Password:
Conferma password
Reinserisci password:
Conferma password
Opzioni e-mail:
Invia tutti i messaggi
Creato il:
Accedi (account creato precedentemente)
Registra dopo (la registrazione è obbligatoria)
Per avere maggiori informazioni su ogni opzione mostrata nell'Interfaccia Utente di BitDefender, muovere il mouse sulla finestra. Un testo di aiuto dettagliato verrà visualizzato in questa area.
Annulla
Indietro
Termina

Creazione Account

Se non si desidera creare un account BitDefender al momento, selezionare **Registra più tardi** e fare clic su **Termina**. Altrimenti, procedere secondo la vostra situazione attuale:

- «Non possiedo un account BitDefender» (p. 349)
- «Ho già un account BitDefender» (p. 350)

Non possiedo un account BitDefender

Per creare correttamente un account BitDefender, seguire questi passaggi:

1. Selezionare **Crea un nuovo account**.
2. Digitare le informazioni richieste nei campi corrispondenti. I dati che fornite qui resteranno riservati.
   - **E-mail** - inserire il tuo indirizzo mail.

- **Password** - inserire una password per il vostro account BitDefender. La password deve essere lunga tra 6 e 16 caratteri.
- **Confermare Password** - inserire di nuovo la password specificata previamente.

Nota
Una volta che l'account è attivato, è possibile utilizzare l'indirizzo e-mail fornito e la password per accedere all'account all'indirizzo http://myaccount.bitdefender.com.

3. A tua scelta, BitDefender puo' informarti su offerte speciali e promozioni usando l'indirizzo mail del tuo account. Selezionare una delle opzioni disponibili dal menu:
   - **Inviatemi tutti i messaggi**
   - **Inviatemi solo i messaggi relativi ai prodotti**
   - **Non inviatemi alcun messaggio**
4. Fare clic su **Crea**.
5. Fare clic su **Termina** per completare l'assistente.
6. **Attivare l'account.** Prima di poter utilizzare l'account, è necessario attivarlo. Controllare l'e-mail e seguire le istruzioni nel messaggio e-mail inviato dal servizio di registrazione BitDefender.

Ho già un account BitDefender

BitDefender rileverà automaticamente se avete già registrato un account BitDefender sul vostro computer. In questo caso, fornire la password per l'account e fare clic su **Accedi**. Fare clic su **Termina** per completare l'assistente.

Se si dispone già di un account attivo, ma BitDefender non lo rileva, seguire questi passi per registrare il prodotto per tale account:

1. Selezionare **Accedi (account creato precedentemente)**.
2. Digitare l'indirizzo e-mail e la password per l'account nei campi corrispondenti.

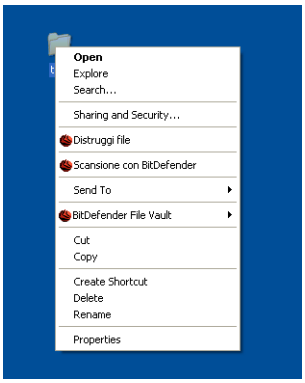
Nota
Se avete dimenticato la vostra password, cliccate su **Password dimenticata?** e seguire le istruzioni.

3. A tua scelta, BitDefender puo' informarti su offerte speciali e promozioni usando l'indirizzo mail del tuo account. Selezionare una delle opzioni disponibili dal menu:
   - **Inviatemi tutti i messaggi**
   - **Inviatemi solo i messaggi relativi ai prodotti**
   - **Non inviatemi alcun messaggio**
4. Fare clic su **Accedi**.
5. Fare clic su **Termina** per completare l'assistente.

Integrazione in Software Windows e di terzi

31. Integrazione nel Menu Contestuale Windows

Il menu contestuale Windows appare ogni volta che si fa clic con il pulsante destro su un file o una cartella del computer o un oggetto sul desktop.



Menu Contestuale Windows

BitDefender si integra nel menu contestuale Windows per aiutare a scansionare facilmente file alla ricerca di virus e prevenire altri utenti da accedere ai file privati. È possibile individuare velocemente opzioni BitDefender sul menu contestuale cercando l'icona BitDefender.

- Scansiona con BitDefender
- BitDefender File Vault
- Distruggi file

31.1. Scansiona con BitDefender

È semplice eseguire la scansione di file, cartelle e persino dischi rigidi interi utilizzando il menu contestuale Windows. Fare clic con il pulsante destro del mouse sull'oggetto che si desidera scansionare e selezionare dal menu **Scansiona con BitDefender**. Lo Scanner BitDefender apparirà e vi guiderà attraverso il processo di scansione.

Opzioni di scansione. Le opzioni di scansione sono preconfigurate per i migliori risultati di scansione. Se vengono individuati fili infetti, BitDefender cercherà di disinfettarli (rimuovere il codice malware). Se la disinfettazione non riesce, la procedura guidata Antivirus Scan consentirà di specificare altre azioni da intraprendere sui file infetti.

Per modificare le opzioni di scansione, seguire questi passaggi:

1. Aprire BitDefender e passare l'interfaccia utente in Modalità Avanzata.
2. Clicca su **Antivirus** dal menù a sinistra.
3. Fare clic sulla scheda **Scansione Virus**.
4. Fare clic con il tasto destro sull'attività **Scansione contestuale** e selezionare **Apri**. Apparirà una finestra.
5. Fare clic su **Personalizza** e configurare le opzioni di scansione come necessario. Per scoprire cosa fa una opzione, posizionare il mouse su di essa e leggere la descrizione visualizzato nel fondo della finestra.
6. Selezionare **Applica** per salvare le modifiche.
7. Fare clic su**OK** per confermare e applicare le nuove opzioni di scansione.

Importante

Non si dovrebbero modificare le opzioni di scansione di questo metodo di scansione a meno che non vi siano ragioni valide per farlo.

31.2. Criptazione File (File Vault) BitDefender

BitDefender File Vault aiuta ad archiviare in modo sicuro i documenti confidenziali sul computer tramite l'uso di file vault.

- Il file vault è uno spazio sicuro dove immagazzinare informazioni personali o file sensibili.
- Il file vault è un file criptato sul vostro computer con estensione bvd. Siccome è criptato, i dati al suo interno sono invulnerabili a furti o a violazioni di sicurezza.
- Quando aprite questo file bvd, apparirà una nuova partizione logica (un nuovo drive). Vi sarà più facile capire questo processo se pensate ad uno simile: aprire un'immagine ISO come CD virtuale.

  Aprire Risorse del Computer e vedrete un nuovo drive basato sulla vostra criptazione file. In esso sarete in grado di fare operazioni sui file (copiare, cancellare, modificare, etc). I file saranno protetti finchè risiederanno in questo drive (perchè viene richiesta una password per l'operazione di apertura).

  Quando avrete finito, bloccare (smontare) il file per comminciare a proteggere il suo contenuto.

È possibile individuare facilmente file vault BitDefender sul computer tramite l'icona BitDefender e l'estensione `.bvd`.

Nota

Questa sezione mostra come creare e gestire file vault BitDefender usando solo opzioni del menu contestuale Windows. È possibile inoltre creare e gestire file vault direttamente dall'interfaccia BitDefender.

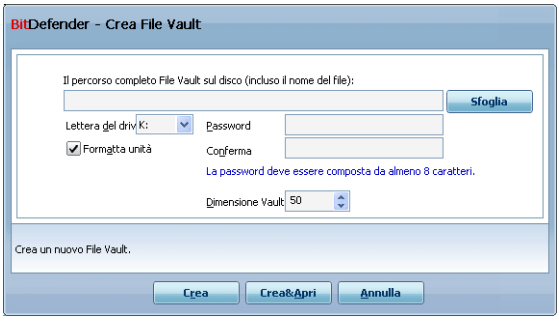
- In Modalità Intermedia andare alla scheda Archiviazione File e utilizzare le opzioni dall'area **Attività Veloci**. Una procedura guidata ti aiuterà a completare ogni attività.
- Per un approccio più diretto, passare l'interfaccia utente in Modalità Avanzata e fare clic su **Criptazione** dal menu a sinistra. Sulla scheda Criptazione File, è possibile vedere e gestire i file vault esistenti e il loro contenuto.

31.2.1. Crea Vault

Tenere a mente che un vault è di fatto solo un file con una estensione `.bvd`. Solo quando si apre il vault, appare un'unità disco virtuale in Risorse del computer ed è possibile archiviare in modo sicuro file al suo interno. Quando si crea un vault, è necessario specificare dove e con quale nome salvarlo sul computer. Inoltre è necessario specificare una password per proteggerne il contenuto. Solo utenti che conoscono la password possono aprire il vault e accedere a documenti e dati in esso archiviati.

Per creare un vault, eseguire questi passi:

1. Fare clic con il pulsante destro sul desktop o su una cartella del computer, puntare su **File Vault BitDefender** e selezionare **Crea File Vault**. Apparirà la finestra seguente:



Crea File Vault

2. Specificare la posizione ed il nome del vault.
   - Cliccare su **Sfoglia**, selezionare la posizione del vault e salvare il file sotto il nome desiderato.
   - È sufficiente digitare il nome del vault nel campo corrispondente per crearlo in Documenti. Per aprire i Documenti, fare clic su start menu Start di Windows e poi **Documenti**.
   - Digitare il percorso completo del vault sul disco. Ad esempio, `C:\my_vault.bvd`.

3. Scegliere una lettera dal menu per il drive. Quando aprite il vault, un disco virtuale con la lettera selezionata apparirà su Risorse del Computer.
4. Digitare la password desiderata per il vault nei campi **Password** e **Conferma**. Qualsiasi persona che tenti di aprire il vault ed accedere ai suoi file, dovrà fornire la password.
5. Selezionare **Formattare drive** per formattare il disco virtuale assegnato al vault. È necessario formattare l'unità prima che si possa aggiungere file al vault.
6. Se desiderate cambiare la dimensione predefinita del vault (50 MB), digitare il valore desiderato nel campo **Dimensione del Vault**.
7. Cliccare su **Creare** se desiderate creare solo il vault nella destinazione selezionata. Per creare e mostrare il vault come un disco virtuale nelle Risorse del Computer, cliccare su **Creare & Aprire** .

BitDefender informerà immediatamente sul risultato dell'operazione. Se si verifica un errore, utilizzare il messaggio di errore per risolvere l'errore. Selezionare **OK** per chiudere la finestra.

Nota

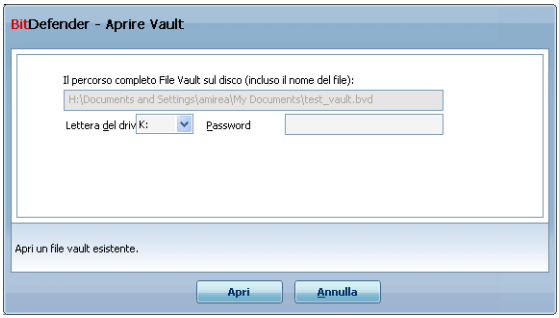
Potrebbe essere conveniente salvare tutti i file vault nella stessa posizione. In questo modo, è possibili trovarli più velocemente.

31.2.2. Apri Vault

Per accedere e lavorare sui file immagazzinati in un vault, dovrete aprire il vault. Quando aprite un vault, apparirà un disco virtuale nelle Risorse del Computer. Il drive avrà la lettera di disco assegnata al vault.

Per aprire un vault, eseguire questi passi:

1. Individuare sul computer il `.bvd` file che rappresenta il vault che si vuole aprire.
2. Fare clic con il pulsante destro sul file, puntare su **BitDefender File Vault** e selezionare **Apri**. Alternative più veloci sarebbero fare un doppio clic sul file, o fare clic con il pulsante di destra e selezionare **Apri**. Apparirà la finestra seguente:



Aprire Vault

3. Scegliere una lettera dal menu per il drive.
4. Digitare la password per il vault nel campo **Password**.
5. Cliccare **Aprire**.

BitDefender informerà immediatamente sul risultato dell'operazione. Se si verifica un errore, utilizzare il messaggio di errore per risolvere l'errore. Selezionare **OK** per chiudere la finestra.

31.2.3. Blocca Vault

Quando abbiate finito di lavorare in un vault, dovrete bloccarlo per proteggere i vostri dati. Bloccando la vault, l'unità disco virtuale corrispondente sparisce da Risorse del computer. Di conseguenza l'accesso ai dati archiviati nel vault è completamente bloccato.

Per bloccare un vault, eseguire questi passi:

1. Aprire Documenti (fare clic su start menu Start di Windows e poi **Risorse del computer**).
2. Identifica l'unità disco virtuale corrispondente al vault che si vuole chiudere. Cercare la lettera dell'unità assegnata al vault quando lo si è aperto.
3. Fare clic con il pulsante destro sull'unità disco virtuale corrispondente, puntare su **BitDefender File Vault** e fare clic su **Chiudi**.

E' anche possibile fare clic con il tasto destro sul file `.bvd` che rappresenta il vault, puntare su **File Vault BitDefender** e fare clic su **Chiudi**.

BitDefender informerà immediatamente sul risultato dell'operazione. Se si verifica un errore, utilizzare il messaggio di errore per risolvere l'errore. Selezionare **OK** per chiudere la finestra.

Nota

Se sono aperti diversi vault, si consiglia di usare l'interfaccia Modalità Avanzata BitDefender. Se si fa clic sulla scheda **Criptazione**, Criptazione File, è possibile vedere una tabella che fornisce informazioni sui vault esistenti. Queste informazioni includono l'eventuale apertura del vault e, in tal caso, la lettera assegnata all'unità.

31.2.4. Aggiungi a file vault

Prima che sia possibile aggiungere file o cartelle ad un vault, è necessario aprire il vault. Una volta che il vault è aperto, è possibile archiviare facilmente file o cartelle all'interno per utilizzare il menu contestuale. Fare clic con il pulsante destro sul file o cartella che si vuole copiare nel vault, puntare su **File Vault BitDefender** e fare clic su **Aggiungi al File Vault**.

- Se solo un vault è aperto, il file o la cartella è copiata direttamente a quel vault.
- Se diversi vault sono aperti, verrà chiesto di scegliere il vault in cui copiare l'elemento. Selezionare dal menu la lettera dell'unità corrispondente al vault desiderato e fare clic su **OK** per copiare l'elemento.

È inoltre possibile utilizzare l'unità disco virtuale corrispondente al vault. Attenersi alla seguente procedura:

1. Aprire Documenti (fare clic su start menu Start di Windows e poi **Risorse del computer**).
2. Inserire l'unità disco virtuale corrispondente al vault. Cercare la lettera dell'unità assegnata al vault quando lo si è aperto.
3. Copia e incolla e trascina file e cartelle direttamente a questa unità disco virtuale.

31.2.5. Rimuovi dal file vault

Per rimuovere i file o cartelle da un vault, il vault deve essere aperto. Per rimuovere file o cartelle da un vault, eseguire questi passi:

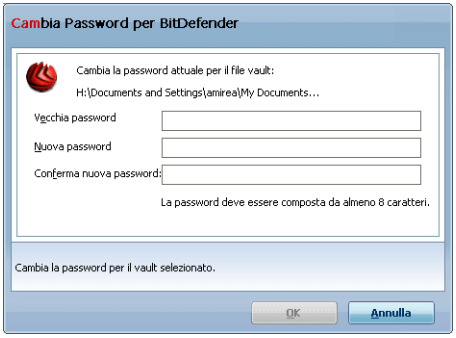
1. Aprire Documenti (fare clic su start menu Start di Windows e poi **Risorse del computer**).
2. Inserire l'unità disco virtuale corrispondente al vault. Cercare la lettera dell'unità assegnata al vault quando lo si è aperto.
3. Rimuove file o cartelle come si fa normalmente in Windows (ad esempio, fare clic con il pulsante destro su un file che si vuole eliminare e selezionare **Elimina**).

31.2.6. Cambiare la Password del Vault

La password protegge il contenuto di un vault da accessi non autorizzati. Solo utenti che conoscono la password possono aprire il vault e accedere a documenti e dati in esso archiviati.

Il vault deve essere bloccato prima che si possa cambiare la sua password. er cambiare la password di un vault, eseguire questi passi:

1. Individuare sul computer il `.bvd` file che rappresenta il vault.
2. Fare clic con il pulsante destro sul file, puntare su **File Vault BitDefender** e selezionare **Modifica Password Vault**. Apparirà la finestra seguente:


Cambia Password per BitDefender
Cambia la password attuale per il file vault:
H:\Documents and Settings\amirea\My Documents...
Vecchia password
Nuova password
Conferma nuova password:
La password deve essere composta da almeno 8 caratteri.
Cambia la password per il vault selezionato.
OK
Annulla

Cambiare la Password del Vault

3. Digitare la password corrente del vault nel campo **Vecchia Password**.
4. Digitare la nuova password del vault nei campi **Nuova password** e **Conferma Nuova Password**.

> **Nota**
>
> La password deve essere composta da almeno 8 caratteri. Per avere una password forte, utilizzare una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @).

5. Cliccare su **OK** per cambiare la password.

BitDefender informerà immediatamente sul risultato dell'operazione. Se si verifica un errore, utilizzare il messaggio di errore per risolvere l'errore. Selezionare **OK** per chiudere la finestra.

31.3. Distruggi file

Quando si cancellano file da Windows, di fatto non vengono eliminati dal disco rigido. Di solito i file eliminati finiscono nel Cestino. Il Cestino consente di ripristinare file eliminati, qualora fossero ancora necessari o se l'eliminazione è stata fortuita.

Quando poi si eliminano i file nel Cestino, Windows non è più in grado di "vederli" e non è più possibile ripristinarli. Tuttavia i file eliminati sono ancora nel tuo disco rigido (fino a quando sono sovrascritti da altri file). Cosa più importante, possono

essere recuperati usando software specializzati per il recupero. Usando un tale software, persone malintenzionate che possono accedere al computer possono recuperare dati confidenziali.

Se si desidera rimuovere file confidenziali dal computer, è necessario ben più della semplice funzione **Elimina** in Windows. BitDefender aiuta a distruggere per sempre i file usando il Distruttore di file. Il Distruttore di file rimuove fisicamente i file dal disco rigido impedendo il recupero con un software specializzato.

Usando il menu contestuale Windows, è possibile distruggere velocemente file o cartelle dal computer. Fare clic con il pulsante destro sul file o sulla cartella che si vuole eliminare in modo permanente, selezionare **Distruggi file** e seguire la procedura guidata. Per ulteriori informazioni sulla procedura guidata Distruttore di File, fare riferimento a «*Eliminazione Definitiva dei File*» (p. 322).

32. Integrazione nei Web Browser

BitDefender vi protegge da tentativi di phishing mentre navigate in Internet. Esamina i siti web visitati e vi allerta se ci sono minacce di phishing. Può essere configurata una White List di siti web che non vogliate vengano esaminati da BitDefender.

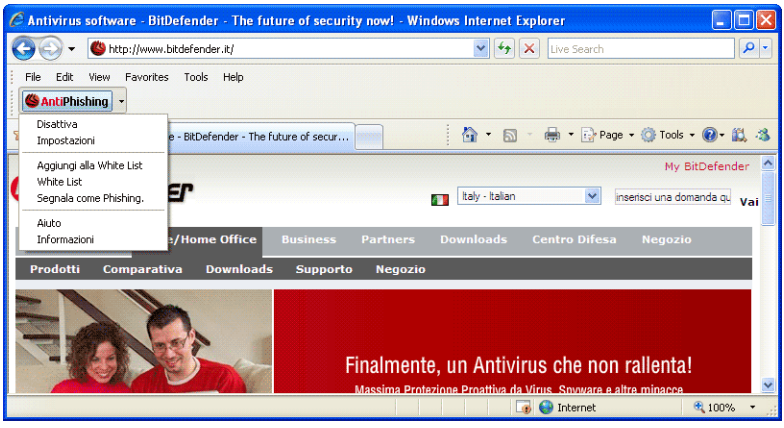
BitDefender si integra direttamente attraverso una barra degli strumenti intuitiva e di facile uso nei seguenti web browser:

- Internet Explorer
- Mozilla Firefox

Potete gestire facilmente ed efficacemente la protezione antiphishing e la White List utilizzando la barra degli strumenti Antiphishing BitDefender integrata nei web browser citati sopra.

La barra degli strumenti antiphishing, rappresentata dall'icona BitDefender, si trova nella parte superiore del browser. Cliccare sopra per aprire il menu della barra degli strumenti.

Nota
Se non potete visualizzare la barra degli strumenti, aprire il menu **Visualizzare**, puntare su **Barre degli strumenti** e selezionare **Barra degli strumenti BitDefender**.



Barra degli Strumenti Antiphishing

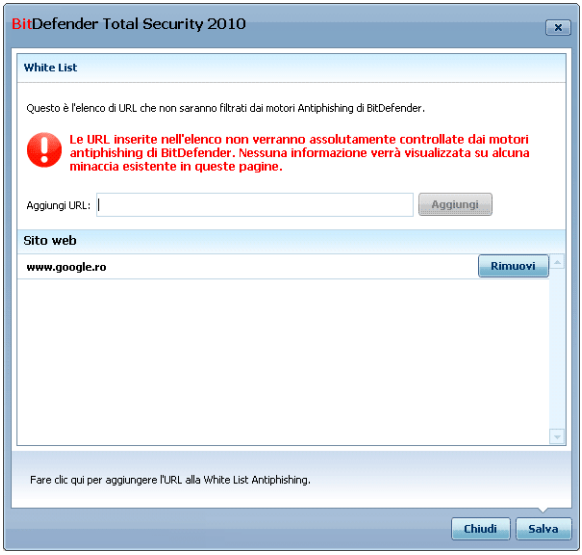
Nella barra degli strumenti sono disponibili i seguenti comandi:

- **Attivare / Disattivare** - attiva / disattiva la protezione Antiphishing di BitDefender nel browser web attuale.

- **Impostazioni** - apre una finestra dove potete specificare le impostazioni della barra degli strumenti Antiphishing. Sono disponibili le seguenti opzioni:
  - **La protezione Web Antiphishing in tempo reale** - individua e avverte in tempo reale se un sito web è oggetto di phishing (impostato per rubare informazioni personali). Questa opzione controlla la protezione antiphishing BitDefender solo nel browser web attuale.
  - **Chiedere prima di aggiungere alla White List** - vi viene chiesto prima di aggiungere un sito web alla White List.
- **Aggiungere alla White List** - aggiunge il sito web corrente alla White List.

> **Nota**
> Aggiungere un sito alla White List significa che BitDefender non esaminerà più il sito per tentativi di phishing. Vi consigliamo di aggiungere alla White List solo siti di cui vi fidate pienamente.

- **White List** - apre la White List.


BitDefender Total Security 2010
White List
Questo è l'elenco di URL che non saranno filtrati dai motori Antiphishing di BitDefender.
Le URL inserite nell'elenco non verranno assolutamente controllate dai motori antiphishing di BitDefender. Nessuna informazione verrà visualizzata su alcuna minaccia esistente in queste pagine.
Aggiungi URL:
Aggiungi
Sito web
www.google.ro
Rimuovi
Fare clic qui per aggiungere l'URL alla White List Antiphishing.
Chiudi
Salva

White List Antiphishing

Potete vedere la lista di tutti i siti web che non vengono controllati dai motori di antiphishing BitDefender. Se si vuole rimuovere un sito dalla White List in modo che sia notificata qualsiasi minaccia di phishing su quella pagina, fare clic sul pulsante **Rimuovi** a fianco.

Potete aggiungere i siti di cui vi fidate pienamente alla White List, in modo che non verranno più esaminati dai motori antiphishing. Per aggiungere un sito alla White List, inserire il suo indirizzo nel campo corrispondente e quindi cliccare **Aggiungere**.

- **Segnala come phishing** - informa il Laboratorio BitDefender che si considera il relativo sito web come sito usato per phishing. Segnalando siti web di phishing si aiuta a proteggere altri da furti di identità.
- **Aiuto** - apre la documentazione elettronica.
- **Informazioni** - apre una finestra nella quale è possibile visualizzare delle informazioni su BitDefender e cercare aiuto nel caso in cui accada qualcosa di inaspettato.

33. Integrazione in Programmi Instant Messenger

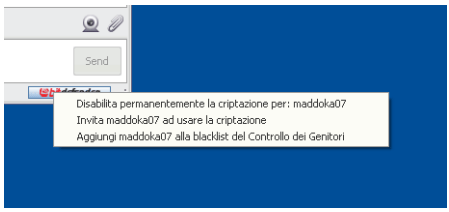
BitDefender offre delle capacità di criptazione per proteggere i vostri documenti confidenziali e le vostre conversazioni attraverso Yahoo Messenger e MSN Messenger.

Di default, BitDefender esegue la criptazione di tutte le vostre sessioni chat, purché:

- Il tuo partner di chat abbia una versione di BitDefender installata che supporti la Criptazione Chat, e la Criptazione Chat sia abilitata per l'applicazione usata per chattare.
- Tu ed il tuo partner di chat usate entrambi Yahoo Messenger o Windows Live (MSN) Messenger.

Importante
BitDefender non eseguirà la criptazione di una conversazione se uno dei partner utilizza un'applicazione chat su web, come Meebo, o altra applicazione chat che supporti Yahoo Messenger o MSN.

Potete configurare facilmente la criptazione dell'instant messaging utilizzando la barra degli strumenti di BitDefender nella finestra di chat. La barra degli strumenti dovrebbe essere posizionata in basso a destra della finestra chat. Cercare il logo BitDefender per trovarla.


Send
Disabilita permanentemente la criptazione per: maddoka07
Invita maddoka07 ad usare la criptazione
Aggiungi maddoka07 alla blacklist del Controllo dei Genitori
Barra degli strumenti BitDefender

Nota
La barra degli strumenti indicate che una conversazione è criptata mostrando una piccola chiave vicino al logotipo BitDefender.

Facendo clic sulla barra degli strumenti di BitDefender appaiono le seguenti opzioni:

- **Disabilita criptazione per sempre per contatto.**
- **Invita contatto ad usare la criptazione.** Per criptare le conversazioni, il contatto deve installare BitDefender e utilizzare un programma IM compatibile.
- **Aggiungi contatto alla blacklist Controllo genitori.** Se si aggiunge un contatto alla blacklist Controllo genitori e il Controllo genitori è abilitato, non si vedranno più i messaggi chat inviati da tale contatto. Per rimuovere il contatto dalla blacklist, fare clic sulla barra degli strumenti e selezionare **Rimuovi contatto dalla blacklist Controllo genitori**.

34. Integrazione nei client di posta

Sicurezza totale BitDefender 2010 include un modulo Antispam. Antispam verifica i messaggi e-mail che si ricevono e identifica quelli che sono spam. I messaggi spam rilevati da BitDefender sono marcati con il prefisso [SPAM] nell'oggetto.

Nota
È fornita una protezione antispam per tutti i client di posta POP3/SMTP.

BitDefender si integra direttamente attraverso una barra degli strumenti intuitiva e di facile uso nei seguenti client di posta:

- Microsoft Outlook
- Outlook Express
- Windows Mail
- Mozilla Thunderbird

BitDefender sposta automaticamente messaggi spam ad una cartella specifica, come segue:

- In Microsoft Outlook, i messaggi spam sono spostati nella cartella **Spam**, situata nella cartella **Posta eliminata**. La cartella **Spam** è creata durante l'installazione di BitDefender.
- In Outlook Express e Windows Mail, i messaggi spam sono spostati direttamente nella cartella **Posta eliminata**.
- In Mozilla Thunderbird, i messaggi spam sono spostati nella cartella **Spam**, situata nella cartella **Cestino**. La cartella **Spam** è creata durante l'installazione di BitDefender.

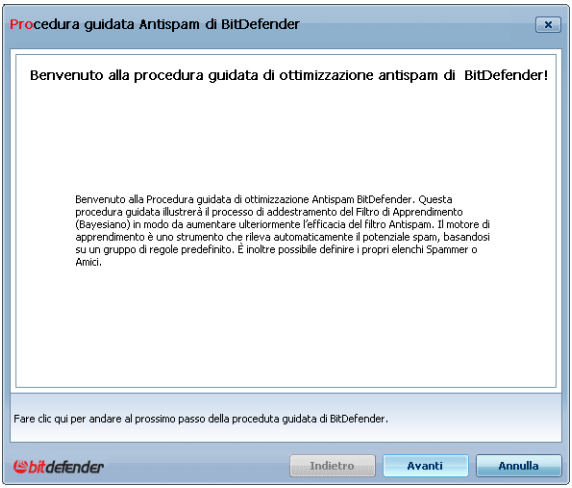
Se si utilizza un altro client per la posta, è necessario creare una regola per spostare i messaggi e-mail segnati come [SPAM] da BitDefender in una cartella personalizzata di quarantena.

34.1. Assistente per la Configurazione Antispam

La prima volta che lanciate il vostro client di posta con BitDefender installato, apparirà l'assistente per aiutarvi a configurare l' Elenco Amici, l' Elenco Spammers e per istruire il Filtro Bayesiano in modo da aumentare l'efficienza dei filtri Antispam.

Nota
La procedura guidata può essere lanciata quando si vuole facendo clic sul pulsante **Procedura guidata** nella barra degli strumenti Antispam.

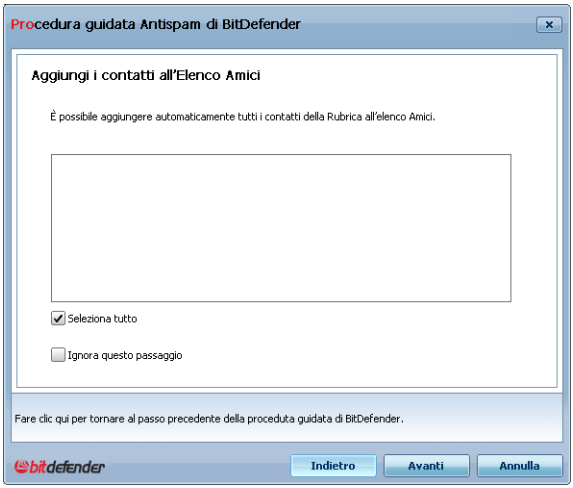
34.1.1. Passo 1/6 - Finestra di Benvenuto


Procedura guidata Antispam di BitDefender
Benvenuto alla procedura guidata di ottimizzazione antispam di BitDefender!
Benvenuto alla Procedura guidata di ottimizzazione Antispam BitDefender. Questa procedura guidata illustrerà il processo di addestramento del Filtro di Apprendimento (Bayesiano) in modo da aumentare ulteriormente l'efficacia del filtro Antispam. Il motore di apprendimento è uno strumento che rileva automaticamente il potenziale spam, basandosi su un gruppo di regole predefinito. È inoltre possibile definire i propri elenchi Spammer o Amici.
Fare clic qui per andare al prossimo passo della proceduta guidata di BitDefender.
bitdefender
Indietro
Avanti
Annulla

Finestra di benvenuto

Selezionare **Avanti**.

34.1.2. Passo 2/6 - Compilare l' Elenco Amici


Procedura guidata Antispam di BitDefender
Aggiungi i contatti all'Elenco Amici
È possibile aggiungere automaticamente tutti i contatti della Rubrica all'elenco Amici.
Seleziona tutto
Ignora questo passaggio
Fare clic qui per tornare al passo precedente della proceduta guidata di BitDefender.
bitdefender
Indietro
Avanti
Annulla

Compilare l' Elenco Amici

Da qui è possibile vedere tutti gli indirizzi della vostra **Rubrica**. Selezionare quelli che si desidera aggiungere al vostro **elenco Amici** (suggeriamo di selezionarli tutti). Si riceveranno tutti i messaggi e-mail provenienti da questi indirizzi, indipendentemente dal loro contenuto.

Per aggiungere tutti i vostri contatti all'elenco degli Amici, selezionare **Selezionare tutti**.

Se si desidera ignorare questo passaggio di configurazione, selezionare **Ignora questo passaggio**. Selezionare **Successivo** per continuare.

34.1.3. Passo 3/6 - Cancellare il Database Bayesiano

Procedura guidata Antispam di BitDefender
Addestra il filtro di apprendimento (Bayesian) di BitDefender
Se l'Antispam di BitDefender non funziona correttamente, consigliamo di "ri-allenare" il filtro Bayesiano. Per farlo è necessario pulire il filtro precedente.
Cancella il database del filtro Antispam
Puoi scegliere di salvare il filtro bayesiano prima di cancellarlo.
Salva Bayes
Carica Bayes
Selezionare questa opzione solo se il filtro antispam è molto impreciso. Nelle fasi successive verrà illustrato come riaddestrare il motore bayesiano (di apprendimento).
Ignora questo passaggio
Fare clic qui per cancellare la procedura guidata e tornare all'operazione precedente.
bitdefender
Indietro
Avanti
Annulla

Cancellare il Database Bayesiano

Nel tempo, si potrà notare che il vostro Filtro Antispam comincia ad essere meno efficace. Il motivo potrebbe essere quello di un addestramento improprio (ovvero nel caso in cui si sia erroneamente marcato un certo numero di messaggi legittimi come Spam e viceversa). Se il vostro filtro risulta essere molto in accurato, potrebbe essere necessario pulire il database del filtro e addestrare nuovamente il filtro seguendo le fasi successive di questa guida.

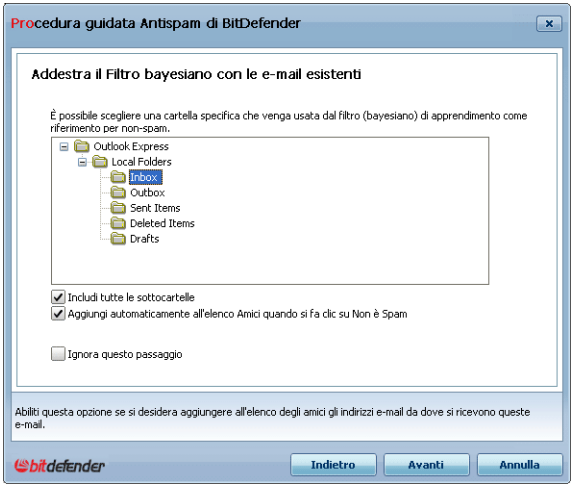
Selezionare **Pulisci il database del filtro antispam** se si desidera impostare nuovamente il database Bayesiano.

E' possibile salvare il database Bayesiano su un file in modo da poterlo utilizzare con un altro prodotto BitDefender o dopo aver reinstallato BitDefender. Per salvare il database Bayesiano, fare clic sul pulsante **Salva Bayes** e salvare nella posizione desiderata. Il file avrà estensione `.dat`.

Per caricare un database Bayesiano precedentemente salvato, fare clic sul pulsante **Carica Bayes** e aprire il file corrispondente.

Se si desidera ignorare questo passaggio di configurazione, selezionare **Ignora questo passaggio**. Selezionare **Successivo** per continuare.

34.1.4. Passo 4/6 - Istruzione del Filtro Bayesiano con messaggi e-mail Leciti


Procedura guidata Antispam di BitDefender
Addestra il Filtro bayesiano con le e-mail esistenti
È possibile scegliere una cartella specifica che venga usata dal filtro (bayesiano) di apprendimento come riferimento per non-spam.
Outlook Express
Local Folders
Inbox
Outbox
Sent Items
Deleted Items
Drafts
Includi tutte le sottocartelle
Aggiungi automaticamente all'elenco Amici quando si fa clic su Non è Spam
Ignora questo passaggio
Abiliti questa opzione se si desidera aggiungere all'elenco degli amici gli indirizzi e-mail da dove si ricevono queste e-mail.
bitdefender
Indietro
Avanti
Annulla

Istruzione del Filtro Bayesiano con messaggi e-mail Leciti

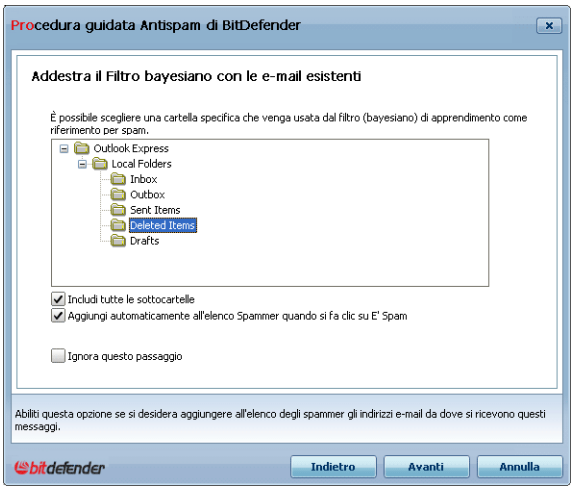
Selezionare una cartella che contenga messaggi e-mail leciti. Questi messaggi verranno utilizzati per addestrare il filtro Antispam.

Ci sono due opzioni avanzate sotto la lista delle directory:

- **Includi sottocartelle** - per includere le sottocartelle nella selezione.
- **Aggiungi automaticamente all'elenco Amici** - per aggiungere i mittenti all'elenco degli Amici.

Se si desidera ignorare questo passaggio di configurazione, selezionare **Ignora questo passaggio**. Selezionare **Successivo** per continuare.

34.1.5. Passo 5/6 - Istruzione del Filtro Bayesiano con SPAM


Procedura guidata Antispam di BitDefender
Addestra il Filtro bayesiano con le e-mail esistenti
È possibile scegliere una cartella specifica che venga usata dal filtro (bayesiano) di apprendimento come riferimento per spam.
Outlook Express
Local Folders
Inbox
Outbox
Sent Items
Deleted Items
Drafts
Includi tutte le sottocartelle
Aggiungi automaticamente all'elenco Spammer quando si fa clic su E' Spam
Ignora questo passaggio
Abiliti questa opzione se si desidera aggiungere all'elenco degli spammer gli indirizzi e-mail da dove si ricevono questi messaggi.
bitdefender
Indietro
Avanti
Annulla

Istruzione del Filtro Bayesiano con SPAM

Selezionare una cartella che contenga messaggi e-mail Spam. Questi messaggi verranno utilizzati per addestrare il filtro Antispam.

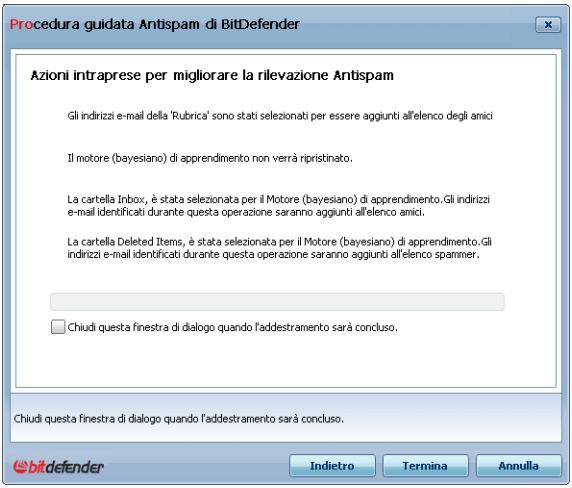
Importante
Assicurarsi che la cartella scelta non contenga assolutamente e-mail lecite, altrimenti la prestazione antispam verrà notevolmente ridotta.

Ci sono due opzioni avanzate sotto la lista delle directory:

- **Includi sottocartelle** - per includere le sottocartelle nella selezione.
- **Aggiungi automaticamente all'elenco Spammer** - per aggiungere i mittenti all'elenco degli Spammer. I messaggi e-mail da questi mittenti verranno sempre identificati come SPAM e trattati di conseguenza.

Se si desidera ignorare questo passaggio di configurazione, selezionare **Ignora questo passaggio**. Selezionare **Successivo** per continuare.

34.1.6. Passo 6/6 – Sommario


Procedura guidata Antispam di BitDefender
Azioni intraprese per migliorare la rilevazione Antispam
Gli indirizzi e-mail della 'Rubrica' sono stati selezionati per essere aggiunti all'elenco degli amici
Il motore (bayesiano) di apprendimento non verrà ripristinato.
La cartella Inbox, è stata selezionata per il Motore (bayesiano) di apprendimento.Gli indirizzi e-mail identificati durante questa operazione saranno aggiunti all'elenco amici.
La cartella Deleted Items, è stata selezionata per il Motore (bayesiano) di apprendimento.Gli indirizzi e-mail identificati durante questa operazione saranno aggiunti all'elenco spammer.
Chiudi questa finestra di dialogo quando l'addestramento sarà concluso.
Chiudi questa finestra di dialogo quando l'addestramento sarà concluso.
bitdefender
Indietro
Termina
Annulla

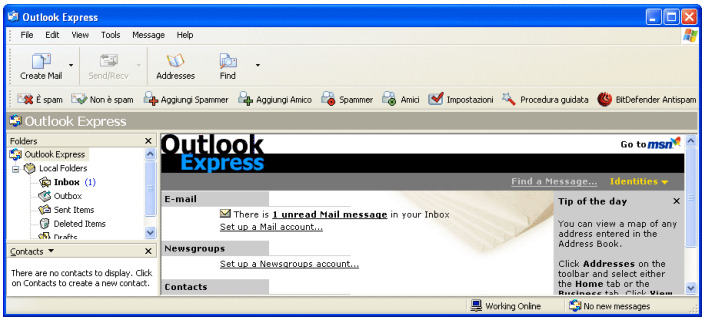
Riassunto

In questa finestra si potranno osservare tutte le impostazioni della guida alla configurazione. Si potrà eseguire qualsiasi modifica ritornando la passo precedente (selezionare **Indietro**).

Se tu non vuoi apportare modifiche, clicca **Fine** per terminare la configurazione.

34.2. Barra degli Strumenti Antispam

Nella parte superiore della finestra del client di posta è possibile vedere la Barra degli Strumenti Antispam. La barra degli strumenti Antispam aiuta a gestire la protezione antispam direttamente dal client di posta. È possibile correggere facilmente BitDefender se segnala un messaggio legittimo come SPAM.



Barra degli Strumenti Antispam

Qui di seguito la spiegazione di ogni pulsante:

- **E' Spam** - invia un messaggio al modulo Bayesiano indicando che la mail selezionata è spam. La mail sarà marcata come SPAM e verrà spostata nella cartella **Spam**.

  I futuri messaggi con caratteristiche uguali verranno marcati come Spam.

  Nota
  E' possibile selezionare uno o più messaggi e-mail come si desidera.

- **Non è Spam** - invia un messaggio al modulo Bayesiano indicando che la mail selezionata non è spam e BitDefender non avrebbe dovuto classificarla come tale. L'e-mail verrà spostata dalla cartella **Spam** alla directory **Inbox**.

  I futuri messaggi con caratteristiche uguali non verranno più marcati come Spam.

  Nota
  E' possibile selezionare uno o più messaggi e-mail come si desidera.

  Importante
  Il pulsante **Non è spam** si attiva quando si seleziona un messaggio marcato come SPAM da BitDefender (normalmente questi messaggi sono situati nella cartella **Spam**).

- **Aggiungi Spammer** - aggiunge il mittente dell'e-mail selezionata all'elenco degli Spammer.

BitDefender aggiungi spammer
BitDefender ha aggiunto il seguente indirizzo all'Elenco Spammer:
mailto:noreply@bitdefender.com
Qualsiasi e-mail ricevuta da questo indirizzo verrà automaticamente spostata nella cartella Spam.
Non mostrare questo messaggio in futuro
OK
Aggiungi Spammer

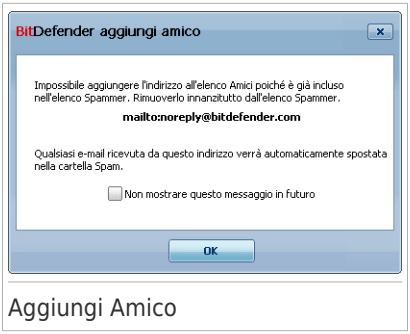
Selezionare **Non mostrare questo messaggio in futuro** se non si desidera la richiesta di conferma quando si aggiunge un indirizzo spammer all'elenco.

Selezionare **OK** per chiudere la finestra.

Le future e-mail provenienti da questo indirizzo verranno marcate come Spam.

Nota
E' possibile selezionare uno o più mittenti e-mail come si desidera.

- **Aggiungi Amici** - aggiunge il mittente dell'e-mail selezionata all'elenco degli Amici.


BitDefender aggiungi amico
Impossibile aggiungere l'indirizzo all'elenco Amici poiché è già incluso nell'elenco Spammer. Rimuoverlo innanzitutto dall'elenco Spammer.
mailto:noreply@bitdefender.com
Qualsiasi e-mail ricevuta da questo indirizzo verrà automaticamente spostata nella cartella Spam.
Non mostrare questo messaggio in futuro
OK
Aggiungi Amico

Selezionare **Non mostrare questo messaggio in futuro** se non si desidera la richiesta di conferma quando si aggiunge un indirizzo di amici all'elenco.

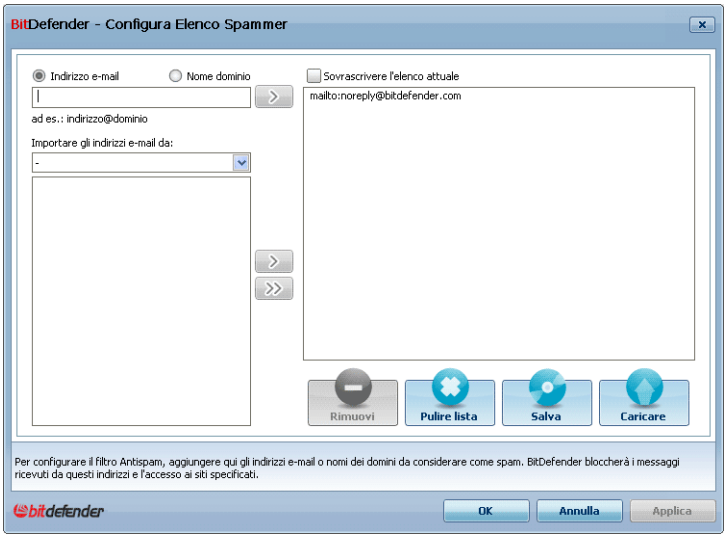
Selezionare **OK** per chiudere la finestra.

Si riceveranno sempre email provenienti da questo indirizzo, indipendentemente dal contenuto del messaggio.

Nota
E' possibile selezionare uno o più mittenti e-mail come si desidera.

- **Spammers** - apre l'**Elenco Spammers**, il quale contiene tutti gli indirizzi mail dai quali non volete ricevere messaggi, indipendentemente dal loro contenuto.

Nota
Qualsiasi mail in arrivo da un indirizzo contenuto nell'**Elenco Spammer** verrà automaticamente marcato come Spam, senza alcun ulteriore processo.



Elenco Spammers

Qui potrete aggiungere o rimuovere elementi dall'**Elenco Spammer**.

Se si desidera aggiungere un indirizzo email, spuntare l' opzione **Indirizzo Email**, digitare l'indirizzo e selezionare il pulsante . L'indirizzo apparirà nell'**Elenco Spammers**.

Importante
Sintassi: name@domain.com.

Se desiderate aggiungere un dominio, selezionare il campo **Dominio**, introdurre il nome e premere il pulsante . Il dominio apparirà nell'**Elenco Spammers**.

Importante
Sintassi:

- @domain.com, *domain.com e domain.com - tutte le mail provenienti da domain.com verranno marcate come Spam;
- *domain* - tutte le mail provenienti da domain (indipendentemente dai suffissi del dominio) verranno marcate come Spam;
- *com - tutte le mail con il suffisso di dominio com verranno marcate come Spam.

Avvertimento

Non aggiungere domini di servizi e-mail legittimi (ad esempio Yahoo, Gmail, Hotmail o altri) all'elenco Spammer. In caso contrario gli indirizzi e-mail ricevuti dagli utenti registrati di tali servizi verranno identificati come spam. Se ad esempio si aggiunge `yahoo.com` all'elenco Spammer, tutti i messaggi e-mail provenienti da indirizzi `yahoo.com` saranno contrassegnati come `[spam]`.

Per importare gli indirizzi e-mail da **Rubrica di Windows** / **Cartelle di Outlook Express** a **Microsoft Outlook** / **Outlook Express** / **Windows Mail** selezionare l'opzione appropriata dal menu a tendina **Importa indirizzi e-mail da**.

Per **Microsoft Outlook Express** / **Windows Mail** apparirà una nuova finestra dove potete selezionare la cartella che contiene gli indirizzi mail che volete aggiungere all'**Elenco Spammer**. Sceglieteli e cliccate su **Seleziona**.

In entrambi i casi gli indirizzi e-mail appariranno nella lista di importazione. Selezionare quelli desiderati e fare clic su per aggiungerli all'**Elenco Spammer**. Facendo clic su tutti gli indirizzi verranno aggiunti all'elenco.

Per rimuovere un elemento dall'elenco, selezionarlo e fare clic su **Rimuovi**. Per eliminare tutti gli elementi dall'elenco fare clic su **Pulisci elenco** e quindi su **Sì** per confermare.

E' possibile salvare l'elenco Spammer in un file in modo da poterlo riutilizzare su un altro computer o dopo aver reinstallato il prodotto. Per salvare l'elenco Spammer, fare clic sul pulsante **Salva** e salvare nella posizione desiderata. Il file avrà estensione `.bwl`.

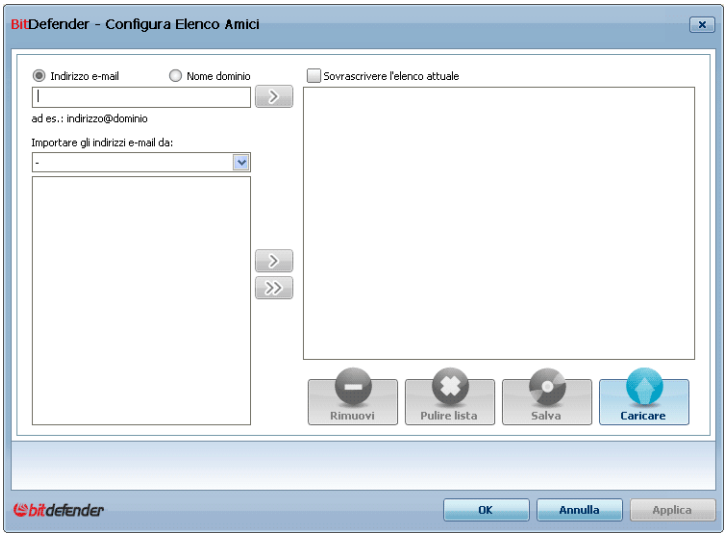
Per caricare un elenco Spammer precedentemente salvato, fare clic sul pulsante **Carica** e aprire il corrispondente file `.bwl`. Per ripristinare il contenuto dell'elenco esistente quando si carica un elenco precedentemente salvato, selezionare **Sovrascrivi l'elenco attuale**.

Selezionare **Applica** e **OK** tper salvare & chiudere **l'Elenco Spammer**.

- **Amici** - apre l'**Elenco Amici** che contiene tutti gli indirizzi mail dai quali volete ricevere sempre i messaggi, indipendentemente dal loro contenuto.

Nota

Qualsiasi mail in arrivo da un indirizzo contenuto nella lista **Elenco Amici**, sarà automaticamente consegnato alla vostra Inbox senza alcun ulteriore processo.



Elenco Amici

Qui potrete aggiungere o rimuovere elementi dall'**Elenco Amici**.

Se si desidera aggiungere un indirizzo email, spuntare il campo **Indirizzo Email**, digitare l'indirizzo e selezionare il pulsante . L'indirizzo apparirà nell'**Elenco Spammers**.

Importante
Sintassi: name@domain.com.

Se desiderate aggiungere un dominio, selezionare l' opzione **Dominio**, digitare il nome e premere il pulsante . Il dominio apparirà nell'**Elenco Amici**.

Importante
Sintassi:

- @domain.com, *domain.com e domain.com - tutte le mail provenienti da domain.com raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;
- *domain* - tutte le mail provenienti da domain (non importa il suffisso del dominio) raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;
- *com - tutte le mail con il suffisso di dominio com raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;

Per importare gli indirizzi e-mail da **Rubrica di Windows** / **Cartelle di Outlook Express** a **Microsoft Outlook** / **Outlook Express** / **Windows Mail** selezionare l'opzione appropriata dal menu a tendina **Importa indirizzi e-mail da**.

Per **Microsoft Outlook Express** apparirà una nuova finestra dove potrete selezionare la cartella che contiene gli indirizzi mail che vorrete aggiungere all'**Elenco Amici**. Sceglierli e cliccare su **Seleziona**.

In entrambi i casi gli indirizzi e-mail appariranno nella lista di importazione. Selezionare quelli desiderati e fare clic su per aggiungerli all'**Elenco Amici**. Facendo clic su tutti gli indirizzi verranno aggiunti all'elenco.

Per rimuovere un elemento dall'elenco, selezionarlo e fare clic su **Rimuovi**. Per eliminare tutti gli elementi dall'elenco fare clic su **Pulisci elenco** e quindi su **Sì** per confermare.

E' possibile salvare l'elenco Amici in un file in modo da poterlo riutilizzare su un altro computer o dopo aver reinstallato il prodotto. Per salvare l'elenco Amici, fare clic sul pulsante **Salva** e salvare nella posizione desiderata. Il file avrà estensione `.bwl`.

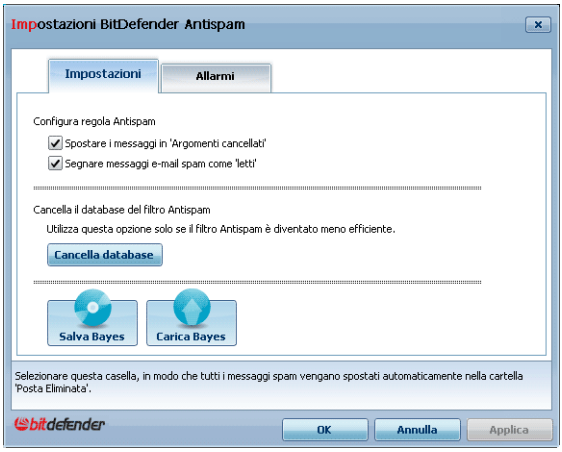
Per caricare un elenco Amici precedentemente salvato, fare clic sul pulsante **Carica** e aprire il corrispondente file `.bwl`. Per ripristinare il contenuto dell'elenco esistente quando si carica un elenco precedentemente salvato, selezionare **Sovrascrivi l'elenco attuale**.

Nota

Raccomandiamo di aggiungere i nomi dei vostri amici e gli indirizzi e-mail all'**elenco Amici**. BitDefender non blocca i messaggi di coloro che sono nell'elenco; aggiungere amici aiuta a garantire che i messaggi leciti vengano recapitati.

Selezionare **Applica** e **OK** per salvare & chiudere **l'Elenco Amici**.

- **Impostazioni** - apre la finestra **Impostazioni** dove potete specificare alcune opzioni per il modulo **Antispam**.


Impostazioni BitDefender Antispam
Impostazioni
Allarmi
Configura regola Antispam
Spostare i messaggi in 'Argomenti cancellati'
Segnare messaggi e-mail spam come 'letti'
Cancella il database del filtro Antispam
Utilizza questa opzione solo se il filtro Antispam è diventato meno efficiente.
Cancella database
Salva Bayes
Carica Bayes
Selezionare questa casella, in modo che tutti i messaggi spam vengano spostati automaticamente nella cartella 'Posta Eliminata'.
bitdefender
OK
Annulla
Applica

Impostazioni

Sono disponibili le seguenti opzioni:

- **Sposta il messaggio in Elementi Cancellati** - sposta i messaggi spam nella cartella **Elementi Cancellati** (solo per Microsoft Outlook Express / Windows Mail);
- **Marcare il messaggio come letto** - per marcare tutti i messaggi Spam come letti così da non essere disturbati quando arrivano nuovi messaggi Spam.

Se il vostro filtro antispam è molto impreciso, può rendersi necessario pulire il database del filtro e addestrare nuovamente il Filtro Bayesiano. Selezionare **Pulisci il database dell'antispam** se si desidera impostare nuovamente il database Bayesiano.

E' possibile salvare il database Bayesiano su un file in modo da poterlo utilizzare con un altro prodotto BitDefender o dopo aver reinstallato BitDefender. Per salvare il database Bayesiano, fare clic sul pulsante **Salva Bayes** e salvare nella posizione desiderata. Il file avrà estensione `.dat`.

Per caricare un database Bayesiano precedentemente salvato, fare clic sul pulsante **Carica Bayes** e aprire il file corrispondente.

Selezionare la tabella **Avvisi** se desiderate accedere alla sezione dove è possibile disattivare la comparsa della finestra di conferma per le opzioni **Aggiungere spammer** ed **Aggiungere amico**.

Nota

Nella finestra **Avvisi** potete anche abilitare / disabilitare la comparsa dell'avviso **Seleziona un messaggio e-mail**. Questo avviso compare quando selezionate un gruppo invece di un messaggio e-mail.

- **Procedura guidata** - apre la Procedura guidata configurazione antispam, ce aiuterà ad addestrare il filtro bayesiano per aumentare ulteriormente l'efficacia del filtraggio BitDefender Antispam. Inoltre è possibile aggiungere indirizzi dall'Agenda all'elenco Amici / Spammer.
- **BitDefender Antispam** - apre l'interfaccia BitDefender.

Come fare

35. Scansione di file e cartelle

La scansione è facile e flessibile con BitDefender. Ci sono 4 modi per impostare BitDefender a scansionare file e cartelle per virus e altro malware:

- Utilizzando il Menu Contestuale Windows
- Utilizzando attività di scansione
- Utilizzando la scansione manuale BitDefender
- Utilizzando la barra attività di scansione

Una volta avviata la scansione, apparirà la procedura guidata di Scansione che illustra il processo. Per ulteriori informazioni sulla procedura guidata, far riferimento a «*Procedura guidata scansione antivirus*» (p. 57).

35.1. Utilizzando il Menu Contestuale Windows

Si tratta del modo più semplice e consigliato per scansionare un file o una cartella sul computer. Fare clic con il pulsante destro del mouse sull'oggetto che si desidera scansionare e selezionare dal menu **Scansiona con BitDefender**. Seguire le istruzioni della procedura guidata Scansione Antivirus per eseguire la scansione.

Tipiche situazioni in cui si userebbe questo metodo includono:

- Si sospetta che un file o una cartella specifica sia infetta.
- Ogni volta che si scarica un file di Internet che potrebbero essere pericolosi.
- Scansionare una condivisione di rete prima di copiare i file sul computer.

35.2. Utilizzando attività di scansione

Se si desidera scansionare il computer o cartelle specifiche regolarmente, si consiglia di considerare l'utilizzo delle attività di scansione. Le attività di scansione istruisce BitDefender in merito a quali ubicazioni scansionare, e quali opzioni di scansione e azioni applicare. Inoltre, è possibile programmare tali azioni per eseguirle regolarmente o in momenti specifici.

Per scansionare il computer utilizzando attività di scansione, è necessario aprire l'interfaccia BitDefender ed eseguire le attività di scansione desiderate. A seconda della modalità di visualizzazione dell'interfaccia, si devono eseguire differenti passi per eseguire attività di scansione.

Esecuzione attività di scansione nella modalità inesperto

Nella modalità inesperto, è possibile eseguire solo una scansione di tutto il computer facendo clic su **Scansiona ora**. Seguire le istruzioni della procedura guidata Scansione Antivirus per eseguire la scansione.

Esecuzione attività di scansione nella modalità intermedia

Nella Modalità Intermedia, è possibile eseguire diverse attività di scansione pre-configurate. È possibile inoltre configurare ed eseguire scansioni personalizzate per scansionare ubicazioni specifiche sul computer usando opzioni di scansione personalizzate. Eseguire questi passi per eseguire una attività di scansione nella Modalità Intermedia:

1. Fare clic sulla scheda **Sicurezza**.
2. Sulla sinistra dell'area Attività veloci, fare clic su **Scansione del sistema** per avviare una scansione standard di tutto il computer. Per eseguire una attività di scansione differente, fare clic sulla freccia sul fondo e selezionare l'attività di scansione desiderata. Per configurare ed eseguire una scansione personalizzata, fare clic su **Scansione Personalizzata**. Queste sono le attività di scansione disponibili:

Funzione di Scansione	Descrizione
Scansione sistema	Esamina l'intero sistema, esclusi gli archivi. Nella configurazione di default la scansione ricerca tutti i tipi di malware ad eccezione dei rootkit.
Scansione del Sistema approfondita	Esamina l'intero sistema. Nella configurazione predefinita, esegue la scansione per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.
Scansione Documenti	Utilizzare questa funzione per esaminare delle cartelle importanti dell'utente corrente: `My Documents`, `Desktop` e `StartUp`. Questo garantirà la sicurezza dei vostri documenti, uno spazio di lavoro sicuro ed applicazioni pulite al avvio.
Personalizzare Scansione	Questa opzione permette di configurare ed eseguire un'attività di scansione personalizzata, permettendo di specificare cosa esaminare e quali opzioni generali di scansione utilizzare. È possibile salvare le attività di scansione personalizzate in modo da poterle utilizzare di nuovo in Modalità Intermedia o Avanzata.

3. Seguire le istruzioni della procedura guidata Scansione Antivirus per eseguire la scansione. Se si sceglie di eseguire una scansione personalizzata, è necessario completare l'assistente Scansione Personalizzata.

Esecuzione attività di scansione in Modalità Avanzata

In Modalità avanzata è possibile eseguire tutte le attività di scansione pre-configurate e modificare le opzioni di scansione. Inoltre è possibile creare attività di scansione personalizzate se si desidera scansionare parti specifiche del computer. Eseguire questi passi per eseguire un'attività di scansione in Modalità Avanzata:

1. Clicca su **Antivirus** dal menù a sinistra.
2. Fare clic sulla scheda **Scansione Virus**. Qui è possibile trovare un numero di attività di scansione di default ed è possibile creare le proprie attività di scansione. Queste sono le attività di scansione predefinite che si possono utilizzare:

Funzione di Default	Descrizione
Scansione del Sistema approfondita	Esamina l'intero sistema. Nella configurazione predefinita, esegue la scansione per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.
Scansione sistema	Esamina l'intero sistema, esclusi gli archivi. Nella configurazione di default la scansione ricerca tutti i tipi di malware ad eccezione dei rootkit.
Scansione Veloce del Sistema	Scansiona le cartelle `Windows` e `Program Files`. Nella configurazione predefinita, esamina per cercare tutti i tipi di malware, esclusi i rootkit, ma non esamina la memoria, il registro nè i cookies.
Documenti	Utilizzare questa funzione per esaminare delle cartelle importanti dell'utente corrente: `My Documents`, `Desktop` e `StartUp`. Questo garantirà la sicurezza dei vostri documenti, uno spazio di lavoro sicuro ed applicazioni pulite al avvio.

3. Fare un doppio clic sull'attività di scansione che si desidera eseguire.
4. Seguire le istruzioni della procedura guidata Scansione Antivirus per eseguire la scansione.

35.3. Utilizzo della Scansione Manuale di BitDefender

La scansione Manuale BitDefender consente di scansionare cartelle o partizioni di disco rigido specifiche senza dover creare una attività di scansione. Questa funzionalità è stata progettata per essere utilizzata quando Windows è in Modalità provvisoria. Se il sistema è infettato con un virus resistente, si può provare a

rimuovere il virus avviando Windows nella Modalità provvisoria e eseguendo la scansione di ogni partizione di disco rigido usando BitDefender Manual Scan.

Per scansionare il computer utilizzando la Scansione Manuale di BitDefender, eseguire i seguenti passi:

1. Sul menu Start di Windows, seguire il percorso **Start → Tutti i programmi → BitDefender 2010 → Scansione manuale di BitDefender** . Apparirà una nuova finestra.
2. Fare clic su **Aggiungi Cartella** per selezionare l'obbiettivo della scansione. Apparirà una nuova finestra.
3. Selezionare il target di scansione:
   - Per eseguire una scansione del desktop, selezionare **Desktop**.
   - Per scansionare un'intera partizione di un disco rigido, selezionarla da Risorse del computer.
   - Per scansionare una cartella specifica, cercare tale cartella e selezionarla.
4. Selezionare **OK**.
5. Fare clic su **Continua** per avviare la scansione.
6. Seguire le istruzioni della procedura guidata Scansione Antivirus per eseguire la scansione.

Cos'è la Modalità provvisoria?
La modalità provvisoria è un modo speciale di avviare Windows, usata principalmente per risolvere problemi che influenzano il normale funzionamento di Windows. Tali problemi vanno da driver in conflitto a virus che impediscono a Windows di avviarsi normalmente. Nella Modalità provvisoria, Windows carica solo una parte minima di componenti del sistema operativo e dei driver fondamentali. Solo alcune applicazioni funzionano nella Modalità provvisoria. Ecco perché la maggior parte del virus sono inattivi quando si utilizza Windows nella Modalità provvisoria e perché possono essere facilmente rimossi.
Per avviare Windows nella Modalità provvisoria, riavviare il computer e premere il tasto F8 fino a quando appare il Menu opzioni avanzate di Windows. È possibile scegliere tra varie opzioni di Windows nella Modalità provvisoria. Si può selezionare **Modalità provvisoria con Networking** per abilitare l'accesso a Internet.

Nota

Per ulteriori informazioni sulla Modalità provvisoria, fare clic su Guida e Supporto tecnico di Windows (nel menu Start, fare clic su **Guida e Supporto tecnico**). È inoltre possibile trovare informazioni utili cercando su Internet.

35.4. Utilizzo della Barra delle Attività di Scansione

La **Barra delle attività di scansione** è una visualizzazione grafica dell'attività di scansione sul vostro sistema. Questa piccola finestra è disponibile per default solo nella Modalità Avanzata.

Barra di Attività della Scansione

Puoi usare la barra di scansione per scansionare velocemente files e cartelle (trascinandoli sopra alla barra) Trascinare il file o la cartella che si desidera scansionare sulla barra delle attività di scansione. Seguire le istruzioni della procedura guidata Scansione Antivirus per eseguire la scansione.

Nota
Per ulteriori informazioni, far riferimento a «*Barra di Attività della Scansione*» (p. 33).

36. Programmazione della scansione del computer

Scansionare il computer periodicamente è il modo migliore per assicurare che il computer non abbia malware. BitDefender consente di programmare attività di scansioni di modo che sia possibile scansionare automaticamente il computer.

Per programmare BitDefender affinché scansioni il computer, eseguire i seguenti passi:

1. Aprire BitDefender e passare l'interfaccia utente in Modalità Avanzata.
2. Clicca su **Antivirus** dal menù a sinistra.
3. Fare clic sulla scheda **Scansione Virus**. Qui è possibile trovare un numero di attività di scansione di default ed è possibile creare le proprie attività di scansione.
   - Le attività di sistema sono disponibili e possono essere eseguite da ogni account utente Windows.
   - Le attività dell'utente sono disponibili solo all'utente che le ha create che è l'unico che le può eseguire.

   Queste sono le attività di scansione predefinite che si possono programmare:

Funzione di Default	Descrizione
Scansione del Sistema approfondita	Esamina l'intero sistema. Nella configurazione predefinita, esegue la scansione per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.
Scansione sistema	Esamina l'intero sistema, esclusi gli archivi. Nella configurazione di default la scansione ricerca tutti i tipi di malware ad eccezione dei rootkit.
Scansione Veloce del Sistema	Scansiona le cartelle `Windows` e `Program Files`. Nella configurazione predefinita, esamina per cercare tutti i tipi di malware, esclusi i rootkit, ma non esamina la memoria, il registro nè i cookies.
Scansione Autologon	Esamina gli elementi che vengono eseguiti quando un utente accede a Windows. Per utilizzare queste attività, è necessario programmarle per farle eseguire all'avvio del sistema. Di default, la scansione autologon è disabilitata
Documenti	Utilizzare questa funzione per esaminare delle cartelle importanti dell'utente corrente: `My Documents`, `Desktop` e `StartUp`. Questo garantirà

Funzione di Default	Descrizione
	la sicurezza dei vostri documenti, uno spazio di lavoro sicuro ed applicazioni pulite al avvio.

Se nessuna di queste scansioni soddisfa le proprie esigenze, è possibile creare una nuova attività di scansione, che è poi possibile programmare per l'esecuzione come necessario.

4. Fare clic sulla attività do scansione desiderata e selezionare **Programma**. Apparirà una nuova finestra.
5. Programmare l'attività per l'esecuzione come necessario:
   - Per eseguire l'attività di scansione solo una volta, selezionare **Una volta** e specificare la data e l'ora di avvio.
   - Per eseguire l'attività di scansione dopo l'avvio del sistema, selezionare **All'avvio del sistema**. Specifica dopo quanto tempo dal suo inizio, il compito deve essere fermato.
   - Per eseguire l'attività di scansione regolarmente, selezionare **Periodicamente** e specificare la frequenza, la data e l'ora di avvio.

   Nota

   Ad esempio, per scansionare il computer ogni sabato alle 2 di notte, è necessario configurare la programmazione nel seguente modo:

   a. Selezionare **Periodicamente**.
   b. Nel campo **Ogni**, digitare 1 e poi selezionare **settimane** dal menu. In questo modo l'attività viene eseguita una volta alla settimana.
   c. Impostare come data di inizio il prossimo sabato.
   d. Impostare come ora di inizio `2:00:00`.

6. Fare clic su **OK** per salvare la programmazione. L'attività di scansione verrà eseguita automaticamente in base alla programmazione definita. Se il computer è spento quando deve essere eseguita la programmazione, l'attività verrà eseguita appena si avvia il computer.

37. Come effettuare il backup dei dati

Con BitDefender Total Secutiry 2010 è possibile creare copie di riserva dei dati più preziosi (documenti, immagini, ecc.) su diversi dispositivi di archiviazione:

- il vostro computer
- un dispositivo di archiviazione USB
- una posizione di rete
- CD/DVD
- un server FTP

Il backup dei dati è utile a proteggersi dalla perdita di dati. Se viene effettuato un backup regolare dei dati, è possibile ripristinarli se necessario. In questo modo è possibile recuperare i file perduti o ritornare ad una versione precedente di un documento.

Importante

BitDefender Total Security 2010 non è progettato per il backup e il ripristino di Windows. Non è possibile creare un'immagine del sistema operativo e delle applicazioni installate in modo da poter ripristinare il sistema in un secondo momento, se necessario.

Per effettuare il backup dei dati su un dispositivo di archiviazione locale, seguire questi passaggi:

1. Apri BitDefender.
2. Avviare l'assistente backup locale.
   - In Modalità Inesperto, area Proteggi il tuo PC, fare clic su **Backup** e selezionare **Backup Locale** dal menu.
   - In Modalità Intermedia, andare alla scheda **Archiviazione File** e fare clic su **Backup Locale**.
   - In Modalità Avanzata, andare su **Backup** e fare clic su **Backup Locale**.
3. Seguire i passaggi della procedura guidata per configurare e creare il backup. Per ulteriori informazioni fare riferimento a *«Assistente Backup Locale»* (p. 76).
   a. Selezionare **Avanti**.
   b. Selezionare i dati di cui si desidera effettuare il backup e fare clic su **Avanti**.
   c. Specificare dove si desidera effettuare il backup dei dati selezionati: selezionare un dispositivo di archiviazione, fare clic su **Scegli posizione** e scegliere la posizione di backup (tranne quando il backup viene effettuato su CD/DVD). Selezionare **Avanti**.
   d. Configurare un programma di backup, se necessario, e fare clic su **Avanti**.
   e. Digitare il nome del lavoro di backup e fare clic su **Avvia Backup**.
   f. Attendere che il backup sia completato e fare clic su **Termina**.

Se sono necessarie ulteriori opzioni di backup, o se si desidera gestire i lavori di backup creati, aprire BitDefender in Modalità Avanzata, andare su **Backup** e fare clic su **Impostazioni**. Per ulteriori informazioni, fare riferimento a «*Impostazioni del Backup*» (p. 283).

38. Come ripristinare i dati di backup

I dati perduti possono essere facilmente recuperati se si è effettuato il backup con BitDefender. Prima di ripristinare tutti i dati, assicurarsi che il dispositivo su cui fai il backup sia disponibile. A seconda del dispositivo è stato utilizzato, potrebbe essere necessario prendere una di queste azioni:

- Inserire il backup della chiavetta USB in una porta USB.
- Inserire il backup CD in un drive CD.
- Verificare se è possibile connettersi alla rete o server FTP dove il backup viene memorizzata.

Per ripristinare i dati di backup salvati su un dispositivo di archiviazione locale, seguire questi passaggi:

1. Apri BitDefender.
2. Avviare l'assistente di ripristino locale.
   - In Modalità Inesperto, area Proteggi il tuo PC, fare clic su **Backup** e selezionare **Ripristino Locale** dal menu.
   - In Modalità Intermedia, andare alla scheda **Archiviazione File**, fare clic sulla freccia sul pulsante **Backup Locale** e selezionare **Ripristino Locale**.
   - In Modalità Avanzata, andare su **Backup** e fare clic su **Ripristino Locale**.
3. Seguire i passaggi della procedura guidata per ripristinare i dati. Per ulteriori informazioni fare riferimento a «*Assistente Recupero Locale*» (p. 81).
   a. Selezionare **Avanti**.
   b. Specificare il file di backup che si desidera ripristinare: selezionare il dispositivo di archiviazione, fare clic su **Scegli posizione** e individuare il file di backup `.ecs`. Selezionare **Avanti**.
   c. Specificare le condizioni di ripristino dei dati e fare clic su **Avanti**. E' possibile scegliere di ripristinare i dati in una posizione differente oppure ripristinare solo dati specifici.
   d. Fare clic su **Ripristina**.
   e. Attendere che i dati siano ripristinati e fare clic su **Termina**.

Se sono necessarie ulteriori opzioni di ripristino dati, o se si desidera gestire i lavori di ripristino creati, aprire BitDefender in Modalità Avanzata, andare su **Backup** e fare clic su **Impostazioni**. Per ulteriori informazioni, fare riferimento a «*Impostazioni del Backup*» (p. 283).

Risoluzione dei problemi e aiuto

39. Risoluzione dei problemi

In questo capitolo vengono spiegati alcuni problemi che si possono incontrare utilizzando BitDefender e vengono inoltre fornite possibili soluzioni per questi problemi. La maggior parte di questi problemi possono essere risolti tramite una configurazione appropriata delle impostazioni del prodotto.

Se non è possibile trovare il problema qui, o se la soluzione fornita non lo risolve, è possibile contattare un rappresentante del supporto tecnico di BitDefender come delineato nel capitolo «*Supporto*» (p. 407).

39.1. Problemi di installazione

Quest'articolo permette di risolvere i problemi di installazione più comuni di BitDefender. Tali problemi possono essere raggruppati nelle seguenti categorie:

- Errori di convalida dell'installazione: non è possibile eseguire l'assistente di setup a causa di condizioni specifiche del sistema.
- Installazione non riuscita: l'installazione è stata avviata dall'assistente di setup ma non è stata completata con successo.

39.1.1. Errori di convalida dell'installazione

Quando viene avviato l'assistente di setup vengono verificate diverse condizioni al fine di convalidare la possibilità di avviare l'installazione. La tabella seguente presenta gli errori di convalida dell'installazione più comuni e le soluzioni per superarli.

Errore	Descrizione e soluzione
Non si dispone di privilegi sufficienti per installare il programma.	Per eseguire l'assistente di setup e installare BitDefender è necessario avere privilegi di amministratore. Eseguire una delle seguenti azioni: ● Accedere ad un account di amministratore di Windows ed eseguire di nuovo l'assistente di setup. ● Fare clic con il pulsante destro sul file di installazione e selezionare **Esegui come**. Digitare il nome utente e la password di un account di amministratore di Windows sul sistema.
Il programma di installazione ha individuato una versione precedente di BitDefender che non è stata disinstallata correttamente.	BitDefender era precedentemente installato sul sistema, ma l'installazione non è stata rimossa completamente. Questa condizione blocca la nuova installazione di BitDefender.

Errore	Descrizione e soluzione
	Per risolvere questo errore ed installare BitDefender, seguire questi passi: 1. Andare su www.bitdefender.it/uninstall e scaricare il programma di disinstallazione sul computer. 2. Eseguire il programma di disinstallazione utilizzando privilegi di amministratore. 3. Riavviare il computer. 4. Avviare di nuovo l'assistente setup per installare BitDefender.
Il prodotto BitDefender non è compatibile con il sistema operativo.	Si sta cercando di installare BitDefender su un sistema operativo non supportato. Controllare i *«Requisiti del sistema»* (p. 2) per scoprire su quali sistemi operativi è possibile installare BitDefender. Se il sistema operativo è Windows XP con Service Pack 1 o senza alcun service pack, è possibile installare il Service Pack 2 o superiore e quindi eseguire di nuovo l'assistente di setup.
Il file di installazione è progettato per un tipo diverso di processore.	Se viene ricevuto tale errore, significa che si sta tentando di eseguire una versione non corretta del file di installazione. Esistono due versioni del file di installazione di BitDefender: una per processori a 32 bit e l'altra per processori a 64 bit. Per assicurarsi di avere la versione corretta per il proprio sistema, scaricare il file di installazione direttamente da www.bitdefender.it.

39.1.2. Installazione non riuscita

Vi sono diverse possibilità di installazione non riuscita:

- Durante l'installazione appare una schermata di errore. Potrebbe essere richiesto di annullare l'installazione oppure potrebbe esservi un pulsante per avviare lo strumento di disinstallazione in modo da pulire il sistema.

Nota
Immediatamente dopo aver avviato l'installazione si potrebbe ricevere una notifica di spazio libero insufficiente su disco per l'installazione di BitDefender. In tal caso liberare lo spazio richiesto sulla partizione dove si desidera installare BitDefender e quindi riprendere o riavviare l'installazione.

- L'installazione si blocca e il sistema potrebbe congelarsi. Solo un riavvio ripristina la capacità di rispondere del sistema.
- L'installazione è stata completata ma è impossibile utilizzare alcune o tutte le funzioni di BitDefender.

Per risolvere un'installazione non riuscita ed installare BitDefender, seguire questi passi:

1. **Ripulire il sistema dopo l'installazione non riuscita.** Se l'installazione non riesce, alcuni file e alcune chiavi di registro di BitDefender potrebbero rimanere sul sistema. Tali rimanenze potrebbero impedire una nuova installazione di BitDefender. Potrebbero inoltre influenzare le prestazioni e la stabilità del sistema. Per questa ragione è necessario rimuoverle prima di tentare nuovamente di installare il prodotto.

   Se la schermata di errore fornisce un pulsante per avviare lo strumento di disinstallazione, fare clic su tale pulsante per ripulire il sistema. Altrimenti procedere nel modo seguente:

   a. Andare su www.bitdefender.it/uninstall e scaricare il programma di disinstallazione sul computer.

   b. Eseguire il programma di disinstallazione utilizzando privilegi di amministratore.

   c. Riavviare il computer.

2. **Controllare le possibili cause per il fallimento dell'installazione.** Prima di procedere con la disinstallazione del prodotto, controllare e rimuovere le possibili condizioni che potrebbero aver causato il fallimento dell'installazione:

   a. Controllare che non vi siano altri programmi di sicurezza installati che potrebbero interferire con il normale funzionamento di BitDefender. Se è così si raccomanda di rimuovere tutti gli altri programmi di sicurezza e quindi installare nuovamente BitDefender.

   b. È anche necessario controllare che il sistema non sia infetto. Eseguire una delle seguenti azioni:

      - Utilizzare il CD di Ripristino di BitDefender per esaminare il computer e rimuovere qualsiasi minaccia esistente. Per ulteriori informazioni fare riferimento a «CD di soccorso BitDefender» (p. 410).

      - Aprire Internet Explorer, andare su www.bitdefender.it ed eseguire una scansione on-line (fare clic sul pulsante **scansione on-line**).

3. Riprovare ad installare BitDefender. Si raccomanda di scaricare ed eseguire la versione più recente del file di installazione da www.bitdefender.it.

4. Se l'installazione non riesce di nuovo, contattare BitDefender per avere assistenza come descritto in «*Supporto*» (p. 407).

39.2. I servizi BitDefender non rispondono

Questo articolo aiuta a risolvere i problemi nel caso in cui *I servizi BitDefender non funzionano*. Si potrebbe trovare questo errore:

- L'icona BitDefender nell'area di notifica è grigia e un pop-up informa che i servizi BitDefender non rispondono.
- La finestra BitDefender mostra che i servizi BitDefender non stanno rispondendo.

L'errore potrebbe essere causato da una delle seguenti condizioni:

- Si sta installando un aggiornamento importante.
- errori temporanei di comunicazione tra i servizi di BitDefender.
- alcuni servizi di BitDefender sono arrestati.
- altri programmi di sicurezza sono in esecuzione sul computer contemporaneamente a BitDefender.
- virus presenti nel sistema stanno interferendo con il normale funzionamento di BitDefender.

Per risolvere questo errore, provare queste soluzione:

1. Aspettare alcuni momenti e vedere se qualcosa cambia. L'errore potrebbe essere temporaneo.
2. Riavviare il computer e aspettare alcuni attimi fino a quando BitDefender è caricato. Aprire BitDefender per vedere se l'errore persiste. Riavviare il computer di solito risolve il problema.
3. Controllare che non vi siano altri programmi di sicurezza installati che potrebbero interferire con il normale funzionamento di BitDefender. Se è così si raccomanda di rimuovere tutti gli altri programmi di sicurezza e quindi installare nuovamente BitDefender.
4. Se l'errore persiste, potrebbe essere un problema più serio (ad esempio, ci potrebbe essere un virus che interferisce con BitDefender). Rivolgersi a BitDefender per supporto come descritto nella sezione «*Supporto*» (p. 407).

39.3. La condivisione file e stampanti sulla Rete Wi-Fi (Wireless) non funziona.

Questo articolo permette di risolvere i seguenti problemi del firewall BitDefender nelle reti Wi-Fi:

- Impossibile condividere i file con i computer sulla rete Wi-Fi.
- Impossibile accedere ad una stampante di rete collegata ad una rete Wi-Fi.
- Impossibile accedere ad una stampante condivisa da un computer sulla rete Wi-Fi.

- Impossibile condividere la propria stampante con i computer sulla rete Wi-Fi.

Prima di iniziare a risolvere tali problemi è necessario comprendere alcuni aspetti della sicurezza e della configurazione del firewall BitDefender con reti Wi-Fi. Dal punto di vista della sicurezza, le reti Wi-Fi rientrano in una delle seguenti categorie:

- **Reti Wi-Fi sicure.** Questo tipo di rete permette la connessione solo di dispositivi Wi-Fi autorizzati. L'accesso alla rete è regolato da una password. Un esempio di reti Wi-Fi sicure è una rete installata in un ufficio.
- **Reti Wi-Fi aperte (non sicure).** Qualsiasi dispositivo Wi-Fi entro il raggio di ricezione di una rete Wi-Fi non sicura può effettuare liberamente la connessione. Le reti Wi-Fi non sicure sono di vasto impiego. Includono praticamente tutte le reti Wi-Fi pubbliche (ad esempio in scuole, internet café, aeroporti e così via). Anche una rete domestica basata su un router wireless non è sicura fino a quando non viene attivata la sicurezza del router.

  Le reti Wi-Fi non sicure presentano un grande rischio per la sicurezza perchè il computer è collegato ad altri computer sconosciuti. Senza l'adeguata protezione fornita da un firewall, chiunque sia collegato alla rete può accedere alle vostre condivisioni e perfino penetrare nel computer.

Quando si è connessi ad una rete Wi-Fi non sicura, BitDefender blocca automaticamente le connessioni con i computer sulla rete. L'accesso a Internet rimane possibile ma non è possibile condividere file o stampanti con altri utenti della rete.

Per abilitare la comunicazione con una rete Wi-Fi, vi sono due soluzioni:

- La soluzione "computer affidabile" permette la condivisione di file e stampanti solo con computer specifici (computer affidabili) sulla rete Wi-Fi. Utilizzare questa soluzione quando si è connessi ad una rete Wi-Fi pubblica (ad esempio a scuola o in un internet café) e si desidera condividere file o stampanti con un amico, oppure si vuole accedere ad una stampante di rete Wi-Fi.
- La soluzione "rete sicura" permette la condivisione di file e stampanti per l'intera rete Wi-Fi (rete sicura). Questa soluzione non è consigliata per motivi di sicurezza, ma può essere utile in determinate situazioni (ad esempio è possibile utilizzarla per una rete Wi-Fi domestica o in ufficio).

39.3.1. Soluzione "Computer Affidabili"

Per configurare il firewall BitDefender in modo da permettere la condivisione di file o stampanti con un computer sulla rete Wi-Fi, o l'accesso ad una stampante di rete Wi-Fi, seguire questi passi:

1. Aprire BitDefender e passare l'interfaccia utente in Modalità Avanzata.
2. Fare clic su **Firewall** nel menu a sinistra.
3. Fare clic sulla scheda **Rete**.

4. Nella tabella Zone, selezionare la rete Wi-Fi e quindi fare clic sul pulsante **Aggiungi**.
5. Selezionare il computer desiderato o la stampante di rete Wi-Fi dall'elenco di dispositivi rilevati sulla rete Wi-Fi. Se tale computer o stampante non è stato rilevato automaticamente, è possibile digitare l'indirizzo IP nel campo **Zona**.
6. Selezionare l'azione **Permetti**.
7. Selezionare **OK**.

Se si continua a non riuscire a condividere i file o la stampante con il computer selezionato, probabilmente la causa non è dovuta al firewall BitDefender sul vostro computer. Controllare altre potenziali cause, ad esempio le seguenti:

- Il firewall dell'altro computer potrebbe bloccare la condivisione di file e stampanti in reti Wi-Fi non sicure (pubbliche).
  - Se il firewall è contenuto in un prodotto BitDefender 2009 o BitDefender 2010, è necessario seguire la stessa procedura sull'altro computer per permettere la condivisione di file e stampanti con il proprio computer.
  - Se viene utilizzato il firewall di Windows, è possibile configurarlo per permettere la condivisione di file e stampanti nel modo seguente: aprire la finestra delle impostazioni di Windows Firewall, scheda **Eccezioni** e selezionare la casella di controllo **Condivisione File e Stampanti**.
  - Se viene utilizzato un altro programma firewall, fare riferimento alla sua documentazione o al file della guida.
- Condizioni generiche che possono impedire l'utilizzo o la connessione ad una stampante condivisa:
  - Potrebbe essere necessario accedere ad un account di amministratore di Windows per poter accedere alla stampante condivisa.
  - Potrebbero essere state impostate delle autorizzazioni per la stampante condivisa che permettono l'accesso solo a specifici computer e utenti. Se si sta condividendo la propria stampante, controllare le autorizzazioni impostate per la stampante per verificare che l'utente dell'altro computer sia autorizzato ad accedere alla stampante. Se si sta provando a collegarsi ad una stampante condivisa, controllare insieme all'utente dell'altro computer di disporre delle autorizzazioni al collegamento alla stampante.
  - La stampante collegata al proprio computer o all'altro computer non è condivisa.
  - La stampante condivisa non è stata aggiunta al computer.

Nota
Per apprendere come gestire la condivisione di stampanti (condividere una stampante, impostare o rimuovere autorizzazioni per una stampante, collegarsi ad una stampante di rete o ad una stampante condivisa) andare alla Guida in Linea

e Supporto Tecnico di Windows (nel menu Start fare clic su **Guida in Linea e Supporto Tecnico**).

Se si continua a non riuscire ad accedere alla stampante di rete Wi-Fi, probabilmente la causa non è dovuta al firewall BitDefender sul vostro computer. L'accesso alla stampante di rete Wi-Fi potrebbe essere ristretto a specifici computer od utenti. Controllare con l'amministratore della rete Wi-Fi se si dispone delle autorizzazioni al collegamento con tale stampante.

Se si ritiene che il problema sia dovuto al firewall BitDefender è possibile contattare BitDefender per avere assistenza come descritto nella sezione «*Supporto*» (p. 407).

39.3.2. Soluzione "Rete Sicura"

Si consiglia di utilizzare questa soluzione solo per reti Wi-Fi domestiche o in ufficio.

Per configurare il firewall BitDefender in modo da permettere la condivisione di file e stampanti con l'intera rete Wi-Fi, seguire questi passi:

1. Aprire BitDefender e passare l'interfaccia utente in Modalità Avanzata.
2. Fare clic su **Firewall** nel menu a sinistra.
3. Fare clic sulla scheda **Rete**.
4. Nella tabella di Configurazione Rete, colonna **Livello di Fiducia**, fare clic sulla freccia nella cella corrispondente alla rete Wi-Fi.
5. A seconda del livello di sicurezza che si desidera ottenere, scegliere una delle seguenti opzioni:
   - **Non sicuro** - per accedere ai file e alle stampanti condivise sulla rete Wi-Fi, senza permettere l'accesso alle proprie condivisioni.
   - **Sicuro** - per permettere la condivisione di file e stampanti in entrambe le direzioni. Questo significa che gli utenti connessi alla rete Wi-Fi possono accedere ai propri file o stampanti condivisi.

Se si continua a non riuscire a condividere i file o la stampante con specifici computer sulla rete Wi-Fi, probabilmente la causa non è dovuta al firewall BitDefender sul vostro computer. Controllare altre potenziali cause, ad esempio le seguenti:

- Il firewall dell'altro computer potrebbe bloccare la condivisione di file e stampanti in reti Wi-Fi non sicure (pubbliche).
  - Se il firewall è contenuto in un prodotto BitDefender 2009 o BitDefender 2010, è necessario seguire la stessa procedura sull'altro computer per permettere la condivisione di file e stampanti con il proprio computer.
  - Se viene utilizzato il firewall di Windows, è possibile configurarlo per permettere la condivisione di file e stampanti nel modo seguente: aprire la finestra delle

impostazioni di Windows Firewall, scheda **Eccezioni** e selezionare la casella di controllo **Condivisione File e Stampanti**.

- Se viene utilizzato un altro programma firewall, fare riferimento alla sua documentazione o al file della guida.

- Condizioni generiche che possono impedire l'utilizzo o la connessione ad una stampante condivisa:
  - Potrebbe essere necessario accedere ad un account di amministratore di Windows per poter accedere alla stampante condivisa.
  - Potrebbero essere state impostate delle autorizzazioni per la stampante condivisa che permettono l'accesso solo a specifici computer e utenti. Se si sta condividendo la propria stampante, controllare le autorizzazioni impostate per la stampante per verificare che l'utente dell'altro computer sia autorizzato ad accedere alla stampante. Se si sta provando a collegarsi ad una stampante condivisa, controllare insieme all'utente dell'altro computer di disporre delle autorizzazioni al collegamento alla stampante.
  - La stampante collegata al proprio computer o all'altro computer non è condivisa.
  - La stampante condivisa non è stata aggiunta al computer.

Nota
Per apprendere come gestire la condivisione di stampanti (condividere una stampante, impostare o rimuovere autorizzazioni per una stampante, collegarsi ad una stampante di rete o ad una stampante condivisa) andare alla Guida in Linea e Supporto Tecnico di Windows (nel menu Start fare clic su **Guida in Linea e Supporto Tecnico**).

Se si continua a non riuscire ad accedere alla stampante di rete Wi-Fi, probabilmente la causa non è dovuta al firewall BitDefender sul vostro computer. L'accesso alla stampante di rete Wi-Fi potrebbe essere ristretto a specifici computer od utenti. Controllare con l'amministratore della rete Wi-Fi se si dispone delle autorizzazioni al collegamento con tale stampante.

Se si ritiene che il problema sia dovuto al firewall BitDefender è possibile contattare BitDefender per avere assistenza come descritto nella sezione «*Supporto*» (p. 407).

39.4. Il filtro Antispam non funziona appropriatamente

Questo articolo permette di risolvere i seguenti problemi delle operazioni di filtro Antispam di BitDefender:

- Un numero di messaggi e-mail legittimi sono contrassegnati come `[spam]`.
- Molti messaggi spam non sono contrassegnati come tali dal filtro antispam.
- Il filtro antispam non rileva nessun messaggio spam.

39.4.1. Messaggi Legittimi sono contrassegnati come [spam]

I messaggi legittimi vengono contrassegnati come `[spam]` semplicemente perchè appaiono come tali al filtro antispam di BitDefender. Normalmente è possibile risolvere questo problema configurando adeguatamente il filtro Antispam.

BitDefender aggiunge automaticamente i destinatari dei messaggi e-mail inviati alla lista degli Amici. I messaggi e-mail ricevuti dai contatti nell'elenco degli Amici sono considerati legittimi. Non vengono verificati dal filtro antispam e di conseguenza non vengono mai contrassegnati come `[spam]`.

La configurazione automatica dell'elenco Amici non impedisce gli errori di rilevamento che possono accadere in queste situazioni:

- Si ricevono molte e-mail commerciali richieste come risultato della sottoscrizione a vari siti web. In questo caso la soluzione è di aggiungere gli indirizzi e-mail da cui si ricevono tali messaggi e-mail all'elenco degli Amici.
- Una parte significativa delle vostre e-mail legittime proviene da individui a cui non avete mai inviato e-mail in precedenza, ad esempio clienti, potenziali partner d'affari o altri. In questo caso sono richieste altre soluzioni.

Se si sta utilizzando uno dei programmi di posta elettronica con cui BitDefender si integra, provare le soluzioni seguenti:

1. Indica errori di rilevamento. Questo è utilizzato per addestrare il Motore di Apprendimento (Bayesiano) del filtro antispam ed aiuta a prevenire futuri errori di rilevamento. Il Motore di Apprendimento analizza i messaggi indicati e ne apprende gli schemi. I successivi messaggi e-mail che corrispondono agli stessi schemi non verranno contrassegnati come `[spam]`.
2. Diminuire il livello di protezione antispam. Diminuendo il livello di protezione, il filtro antispam avrà bisogno di maggiori indicazioni di spam per classificare un messaggio e-mail come spam. Utilizzare questa soluzione solo se molti messaggi legittimi (inclusi i messaggi commerciali richiesti) vengono rilevati scorrettamente come spam.
3. Addestra nuovamente il Motore di Apprendimento (Filtro Bayesiano). Utilizzare questa soluzione solo se le soluzioni precedenti non hanno prodotto risultati soddisfacenti.

Nota

BitDefender si integra nella maggior parte delle applicazioni di posta elettronica comunemente utilizzate per mezzo di una barra degli strumenti antispam di facile utilizzo. Per un elenco completo di applicazioni di posta supportate, fare riferimento a «*Software supportato*» (p. 2).

Se si utilizza un'applicazione di posta differente, non è possibile indicare gli errori di rilevamento ed addestrare il Motore di Apprendimento. Per risolvere il problema provare a diminuire il livello di protezione antispam.

Aggiungi i contatti all'Elenco Amici

Se si sta utilizzando un'applicazione di posta supportata si possono facilmente aggiungere i mittenti dei messaggi legittimi all'elenco degli Amici. Attenersi alla seguente procedura:

1. Nell'applicazione di posta selezionare un messaggio e-mail inviato dal mittente che si desidera aggiungere all'elenco degli Amici.
2. Fare clic sul pulsante **Aggiungi Amico** sulla barra degli strumenti antispam di BitDefender.
3. Può essere richiesto di accettare gli indirizzi aggiunti all'elenco degli Amici. Selezionare **Non mostrare di nuovo questo messaggio** e fare clic su **OK**.

Si riceveranno sempre email provenienti da questo indirizzo, indipendentemente dal contenuto del messaggio.

Se si utilizza un'applicazione di posta differente, è possibile aggiungere i contatti all'elenco degli Amici dall'interfaccia di BitDefender. Attenersi alla seguente procedura:

1. Aprire BitDefender e passare l'interfaccia utente in Modalità Avanzata.
2. Fare clic su **Antispam** nel menu a sinistra.
3. Fare clic sulla scheda **Stato**.
4. Fare clic su **Gestisci Amici**. Apparirà la finestra di configurazione.
5. Digitare l'indirizzo e-mail da cui si desidera sempre ricevere messaggi e-mail e fare clic sul pulsante per aggiungere l'indirizzo all'elenco degli Amici.
6. Selezionare **OK** per salvare le modifiche e chiudere la finestra.

Indica Errori di Rilevamento

Se si sta utilizzando un'applicazione di posta supportata è possibile correggere facilmente il filtro antispam (indicando quali messaggi e-mail non devono essere contrassegnati come `[spam]`). Facendo ciò si migliorerà considerevolmente l'efficienza del filtro antispam. Attenersi alla seguente procedura:

1. Aprire l'applicazione di posta.
2. Andare alla cartella posta indesiderata dove vengono spostati i messaggi spam.
3. Selezionare il messaggio legittimo scorrettamente contrassegnato come `[spam]` da BitDefender.

4. Fare clic sul pulsante **Aggiungi Amico** sulla barra degli strumenti antispam di BitDefender per aggiungere il mittente all'elenco degli Amici. Può essere necessario premere **OK** per confermare. Si riceveranno sempre email provenienti da questo indirizzo, indipendentemente dal contenuto del messaggio.
5. Fare clic sul pulsante **Non è Spam** sulla barra degli strumenti antispam di BitDefender (normalmente posizionata nella parte superiore della finestra del client di posta). Questo indica al Motore di Apprendimento che il messaggio selezionato non è spam. Il messaggio e-mail selezionato verrà spostato nella cartella Inbox. I successivi messaggi e-mail che corrispondono agli stessi schemi non verranno più contrassegnati come `[spam]`.

Diminuzione del Livello di Protezione Antispam

Per diminuire il livello di protezione antispam, seguire questi passaggi:

1. Aprire BitDefender e passare l'interfaccia utente in Modalità Avanzata.
2. Fare clic su **Antispam** nel menu a sinistra.
3. Fare clic sulla scheda **Stato**.
4. Spostare il selettore verso il basso lungo la scala.

Si consiglia di diminuire la protezione di un solo livello ed attendere per un tempo sufficiente a valutarne i risultati. Se molti messaggi e-mail continuano ad essere contrassegnati come `[spam]`, è possibile diminuire ulteriormente il livello di protezione. Se si nota che molti messaggi spam non vengono rilevati, non si dovrebbe diminuire il livello di protezione.

Addestra di nuovo il Motore di Apprendimento (Bayesiano)

Prima di addestrare il Motore di Apprendimento (Bayesiano), preparare una cartella contenente solo messaggi SPAM ed una contenente solo messaggi legittimi. Il Motore di Apprendimento le analizzerà e apprenderà le caratteristiche che definiscono lo spam o i messaggi legittimi che vengono normalmente ricevuti. Affinchè l'addestramento sia efficace devono esservi oltre 50 messaggi per ciascuna categoria.

Per ripristinare il database Bayesiano e addestrare di nuovo il Motore di Apprendimento, seguire questi passaggi:

1. Aprire l'applicazione di posta.
2. Dalla barra degli strumenti antispam di BitDefender fare clic sul pulsante **Wizard** per avviare l'assistente di configurazione antispam. Informazioni dettagliate su questo assistente sono disponibili alla sezione *«Assistente per la Configurazione Antispam»* (p. 364).
3. Selezionare **Avanti**.
4. Selezionare **Ignora questo passaggio** e fare clic su **Avanti**.

5. Selezionare **Svuota il database del filtro antispam** e fare clic su **Avanti**.
6. Selezionare la cartella contenente i messaggi legittimi e fare clic su **Avanti**.
7. Selezionare la cartella contenente i messaggi SPAM e fare clic su **Avanti**.
8. Fare clic su **Termina** per avviare il processo di apprendimento.
9. Quando l'addestramento è completato, fare clic su **Chiudi**.

Chiedere Aiuto

Se questa informazione non è stata utile, è possibile contattare BitDefender per avere assistenza, come descritto alla sezione «*Supporto*» (p. 407).

39.4.2. Molti Messaggi Spam non vengono rilevati

Se si ricevono molti messaggi spam che non vengono contrassegnati come `[spam]`, è necessario configurare il filtro antispam di BitDefender in modo da migliorarne l'efficienza.

Se si sta utilizzando uno dei programmi di posta elettronica con cui BitDefender si integra, provare le soluzioni seguenti, una alla volta:

1. Indica messaggi spam non rilevati. Questo è utilizzato per addestrare il Motore di Apprendimento (Bayesiano) del filtro antispam e di norma migliora il rilevamento antispam. Il Motore di Apprendimento analizza i messaggi indicati e ne apprende gli schemi. I successivi messaggi e-mail che corrispondono agli stessi schemi verranno contrassegnati come `[spam]`
2. Aggiungi spammer all'elenco Spammer. I messaggi e-mail ricevuti dagli indirizzi nell'elenco Spammer sono contrassegnati automaticamente come `[spam]`.
3. Aumentare il livello di protezione antispam. Aumentando il livello di protezione, il filtro antispam avrà bisogno di minori indicazioni di spam per classificare un messaggio e-mail come spam.
4. Addestra nuovamente il Motore di Apprendimento (Filtro Bayesiano). Utilizzare questa soluzione quando il rilevamento dello spam è molto insoddisfacente e l'indicazione di messaggi spam non rilevati non funziona più.

Nota

BitDefender si integra nella maggior parte delle applicazioni di posta elettronica comunemente utilizzate per mezzo di una barra degli strumenti antispam di facile utilizzo. Per un elenco completo di applicazioni di posta supportate, fare riferimento a «*Software supportato*» (p. 2).

Se si utilizza un'applicazione di posta differente, non è possibile indicare gli errori di rilevamento ed addestrare il Motore di Apprendimento. Per risolvere il problema provare a aumentare il livello di protezione antispam e ad aggiungere gli spammer all'elenco Spammer.

Indica Messaggi Spam non rilevati

Se si utilizza un'applicazione di posta supportata si può facilmente indicare quali messaggi e-mail avrebbero dovuto essere rilevati come spam. Facendo ciò si migliora considerevolmente l'efficienza del filtro antispam. Attenersi alla seguente procedura:

1. Aprire l'applicazione di posta.
2. Andare alla cartella Inbox.
3. Selezionare i messaggi di spam non rilevati.
4. Fare clic sul pulsante **E' Spam** sulla barra degli strumenti antispam di BitDefender (normalmente posizionata nella parte superiore della finestra del client di posta). Questo indica al Motore di Apprendimento che i messaggi selezionati sono spam. Vengono immediatamente contrassegnati come `[spam]` e verranno spostati alla cartella posta indesiderata. I successivi messaggi e-mail che corrispondono agli stessi schemi verranno contrassegnati come `[spam]`

Aggungere Spammer all'Elenco Spammer

Se si sta utilizzando un'applicazione di posta supportata si possono facilmente aggiungere i mittenti dei messaggi di spam all'elenco degli Spammer. Attenersi alla seguente procedura:

1. Aprire l'applicazione di posta.
2. Andare alla cartella posta indesiderata dove vengono spostati i messaggi spam.
3. Selezionare i messaggi contrassegnati come `[spam]` da BitDefender.
4. Fare clic sul pulsante **Aggiungi Spammer** sulla barra degli strumenti antispam di BitDefender.
5. Può essere richiesto di accettare gli indirizzi aggiunti all'elenco degli Spammer. Selezionare **Non mostrare di nuovo questo messaggio** e fare clic su **OK**.

Se si sta utilizzando un'applicazione di posta differente è possibile aggiungere manualmente gli spammer all'elenco Spammer dall'interfaccia di BitDefender. Si tratta di un metodo conveniente solo quando si ricevono diversi messaggi spam dallo stesso indirizzo e-mail. Attenersi alla seguente procedura:

1. Aprire BitDefender e passare l'interfaccia utente in Modalità Avanzata.
2. Fare clic su **Antispam** nel menu a sinistra.
3. Fare clic sulla scheda **Stato**.
4. Fare clic su **Gestisci Spammer** Apparirà la finestra di configurazione.
5. Digitare l'indirizzo e-mail dello spammer e fare clic sul pulsante per aggiungere l'indirizzo all'elenco Spammer.
6. Selezionare **OK** per salvare le modifiche e chiudere la finestra.

Aumento del Livello di Protezione Antispam

Per aumentare il livello di protezione antispam, seguire questi passaggi:

1. Aprire BitDefender e passare l'interfaccia utente in Modalità Avanzata.
2. Fare clic su **Antispam** nel menu a sinistra.
3. Fare clic sulla scheda **Stato**.
4. Spostare il selettore verso l'alto lungo la scala.

Addestra di nuovo il Motore di Apprendimento (Bayesiano)

Prima di addestrare il Motore di Apprendimento (Bayesiano), preparare una cartella contenente solo messaggi SPAM ed una contenente solo messaggi legittimi. Il Motore di Apprendimento le analizzerà e apprenderà le caratteristiche che definiscono lo spam o i messaggi legittimi che vengono normalmente ricevuti. Affinchè l'addestramento sia efficace devono esservi oltre 50 messaggi per ciascuna cartella.

Per ripristinare il database Bayesiano e addestrare di nuovo il Motore di Apprendimento, seguire questi passaggi:

1. Aprire l'applicazione di posta.
2. Dalla barra degli strumenti antispam di BitDefender fare clic sul pulsante **Wizard** per avviare l'assistente di configurazione antispam. Informazioni dettagliate su questo assistente sono disponibili alla sezione «*Assistente per la Configurazione Antispam*» (p. 364).
3. Selezionare **Avanti**.
4. Selezionare **Ignora questo passaggio** e fare clic su **Avanti**.
5. Selezionare **Svuota il database del filtro antispam** e fare clic su **Avanti**.
6. Selezionare la cartella contenente i messaggi legittimi e fare clic su **Avanti**.
7. Selezionare la cartella contenente i messaggi SPAM e fare clic su **Avanti**.
8. Fare clic su **Termina** per avviare il processo di apprendimento.
9. Quando l'addestramento è completato, fare clic su **Chiudi**.

Chiedere Aiuto

Se questa informazione non è stata utile, è possibile contattare BitDefender per avere assistenza, come descritto alla sezione «*Supporto*» (p. 407).

39.4.3. Il Filtro Antispam non rileva alcun messaggio spam

Se nessun messaggio spam viene contrassegnato come `[spam]`, potrebbe esserci un problema relativo al filtro Antispam BitDefender. Prima di risolvere questo problema, assicurarsi che non sia causato da una delle seguente condizioni:

- La protezione antispam BitDefender è disponibile solo per client e-mail configurati per ricevere messaggi e-mail tramite il protocollo POP3. Questo vuol dire che:
  - I messaggi e-mail ricevuti tramite servizi e-mail web (ad esempio Yahoo, Gmail, Hotmail o altri) non sono filtrati per spam da BitDefender.
  - Se il proprio client e-mail è configurato per ricevere messaggi e-mail usando un protocollo diverso da POP3 (per esempio, IMAP4), il filtro Antispam BitDefender non verifica se siano spam.

  Nota

  POP3 è uno dei protocolli più usati per scaricare messaggi e-mail da un server di posta. Se non si conosce il protocollo usato dal proprio client e-mail per scaricare messaggi e-mail, chiedere alla persona che ha configurato il proprio client e-mail.

- Sicurezza totale BitDefender 2010 non esegue la scansione del traffico POP3 di Lotus Notes.

Si dovrebbero inoltre verificare le seguenti possibili cause:

1. Assicurarsi che Antispam sia abilitato.
   a. Apri BitDefender.
   b. Fare clic sul pulsante **Impostazioni** in alto a destra.
   c. Nella categoria di impostazioni di sicurezza, verificare lo status antispam.

   Se Antispam è disabilitato, questa è la causa dei problemi. Abilitare Antispam e monitorare il funzionamento dell'antispam per vedere se il problema è risolto.
2. Sebbene non sia molto probabile, si consiglia di verificare se BitDefender è stato configurato per non contrassegnare i messaggi spam come `[spam]`.
   a. Aprire BitDefender e passare l'interfaccia utente in Modalità Avanzata.
   b. Fare clic su **Antispam** sul menu di sinistra e poi sulla scheda **Impostazioni**.
   c. Assicurarsi che l'opzione **Segnare messaggi spam nell'oggetto** sia selezionata.

Una possibile soluzione consiste nel riparare o reinstallare il prodotto. Tuttavia si consiglia di contattare BitDefender per supporto, come descritto nella sezione «*Supporto*» (p. 407).

39.5. Rimozione di BitDefender non riuscita

Questo articolo permette di risolvere gli errori che potrebbero verificarsi nella rimozione di BitDefender. Vi sono due possibili situazioni:

- Durante la rimozione appare una schermata di errore. La schermata fornisce un pulsante per avviare uno strumento di disinstallazione che pulirà il sistema.
- La rimozione si blocca e il sistema potrebbe congelarsi. Fare clic su **Annulla** per annullare la rimozione. Se questo non dovesse funzionare, riavviare il sistema.

Se la rimozione non riesce, alcuni file e alcune chiavi di registro di BitDefender potrebbero rimanere sul sistema. Tali rimanenze potrebbero impedire una nuova installazione di BitDefender. Potrebbero inoltre influenzare le prestazioni e la stabilità del sistema. Per rimuovere completamente BitDefender dal sistema è necessario avviare lo strumento di disinstallazione.

Se la rimozione non riesce con una schermata di errore, fare clic sul pulsante per avviare lo strumento di disinstallazione e ripulire il sistema. Altrimenti procedere nel modo seguente:

1. Andare su www.bitdefender.it/uninstall e scaricare il programma di disinstallazione sul computer.
2. Eseguire il programma di disinstallazione utilizzando privilegi di amministratore. Il tool di disinstallazione rimuoverà tutti i file e chiavi di registro che non siano stati rimossi durante il processo automatico di rimozione.
3. Riavviare il computer.

Se questa informazione non è stata utile, è possibile contattare BitDefender per avere assistenza, come descritto alla sezione «*Supporto*» (p. 407).

40. Supporto

In veste di stimato fornitore, BitDefender si sforza di fornire ai propri clienti un livello senza pari di supporto veloce e accurato. Il centro di conoscenza BitDefender fornisce articoli che contengono soluzioni alla maggior parte dei problemi e delle domande relative a BitDefender. Se non si riesce a trovare una soluzione nel centro di conoscenza BitDefender, è possibile contattare il Servizio clienti BitDefender. Il nostro rappresentate del supporto risponderà alle domande in tempo e vi fornirà tutta l'assistenza necessaria.

40.1. BitDefender Knowledge Base(Archivio D'informazione BitDefender)

L' Archivio D'informazione BitDefender è un deposito d'informazione sui prodotti BitDefender. Conserva, in un formatto facilmente accessibile, rapporti sui risultati del supporto tecnico in corso ed attività di disinfezione dei team di supporto e sviluppo di BitDefender , assieme a più articoli su prevenzione virus, la gestione delle soluzioni BitDefender e spiegazioni dettagliate, e tanti altri articoli.

L'Archivio D'informazione BitDefender è aperto al pubblico e gratuitamente esplorabile. Questa ricchezza d'informazione è un altro modo ancora di fornire ai clienti di BitDefender dalle conoscenze tecniche e comprensione necessarie. Tutte le richieste valide d'informazione o rapporti su difetti, provenienti di clienti di BitDefender trovano prima o poi la loro strada fino al'Archivio D'informazione BitDefender, come rapporti di disinfezione, dei modi di aggirare le truffe, o articoli informativi, in modo di supplementare i file di aiuto dei prodotti.

L' Archivio D'informazione BitDefender è disponibile in qualsiasi momento su http://kb.bitdefender.com.

40.2. Chiedere Aiuto

Per richiedere aiuto, si deve utilizzare il Self-Service Web BitDefender. Eseguire i seguenti passi:

1. Visitare http://www.bitdefender.com/help. Qui è possibile trovare il Centro di conoscenza BitDefender. Il Centro di conoscenza BitDefender include numerosi articoli che contengono soluzioni per questioni relative a BitDefender.
2. Fare una ricerca del Centro di conoscenza BitDefender per articoli che potrebbero fornire una soluzione al problema.
3. Leggere l'articolo pertinente e provare la soluzione proposta.
4. Se questa soluzione non risolve i tuoi problemi, utilizzare il link nell'articolo per contattare il Servizio clienti BitDefender.
5. Accedere all'account di BitDefender.

6. Contatta un rappresentante di supporto BitDefender tramite e-mail, chat o telefono.

40.3. Informazioni di Contatto:

Una comunicazione efficiente è la chiave di un business di successo. Negli ultimi 10 anni BITDEFENDER ha acquisito una reputazione inestimabile superando le aspettative di clienti e partners, sforzandosi costantemente per una comunicazione sempre più efficiente. Se avete delle domande o richieste, non esitare a contattarci.

40.3.1. Indirizzi Web

Dipartimento vendite: sales@bitdefender.com
Supporto tecnico: www.bitdefender.com/help
Documentazione: documentation@bitdefender.com
Programma partner: partners@bitdefender.com
Marketing: marketing@bitdefender.com
Rapporti con i Media: pr@bitdefender.com
Opportunità di lavoro: jobs@bitdefender.com
Invio virus: virus_submission@bitdefender.com
Invio spam: spam_submission@bitdefender.com
Report Abuse: abuse@bitdefender.com
Pagina web del prodotto: http://www.bitdefender.it
Archivi ftp del prodotto: ftp://ftp.bitdefender.com/pub
Distributori locali: http://www.bitdefender.it/site/Partnership/list/
Archivio D'informazione BitDefender: http://kb.bitdefender.com

40.3.2. Uffici BitDefender

Gli uffici (succursali) di BitDefender sono pronti a rispondere a qualunque richiesta riguardo le loro aree di operazioni, in materie commerciale e generale. I loro rispettivi indirizzi e contatti sono elencati sotto.

U.S.A

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Telefono (ufficio&vendite): 1-954-776-6262
Vendite: sales@bitdefender.com
Supporto tecnico: http://www.bitdefender.com/help
Web: http://www.bitdefender.com

Germany

BitDefender GmbH

Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Ufficio: +49 2301 91 84 222
Vendite: vertrieb@bitdefender.de
Supporto tecnico: http://kb.bitdefender.de
Web: http://www.bitdefender.de

UK ed Irlanda

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
Mail: info@bitdefender.co.uk
Telefono: +44 (0) 8451-305096
Vendite: sales@bitdefender.co.uk
Supporto tecnico: http://www.bitdefender.com/help
Web: http://www.bitdefender.co.uk

Spain

BitDefender España SLU
C/ Balmes, 191, 2º, 1ª, 08006
Barcelona
Fax: +34 932179128
Telefono: +34 902190765
Vendite: comercial@bitdefender.es
Supporto tecnico: www.bitdefender.es/ayuda
Sito web: http://www.bitdefender.es

Romania

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
Fax: +40 21 2641799
Telefono vendite: +40 21 2063470
Indirizzo e-mail ufficio vendite: sales@bitdefender.ro
Supporto tecnico: http://www.bitdefender.ro/suport
Sito web: http://www.bitdefender.ro

CD di soccorso BitDefender

41. Panoramica

Sicurezza Internet BitDefender 2010 include un CD di avvio (BitDefender Rescue CD), in grado di eseguire la scansione e di disinfettare tutti i dischi rigidi prima che il Sistema Operativo si avvii.

Dovresti usare il CD di soccorso BitDefender ogni volta che il tuo sistema operativo non lavora correttamente per via di infezioni di virus. Quello succede normalmente quando non usi un prodotto antivirus.

L'aggiornamento delle impronte dei virus è fatta automaticamente, senza l'intervento dell'utente, ogni volta che inizi il CD di soccorso BitDefender.

BitDefender Rescue CD è una distribuzione di Knoppix ri-masterizzato di BitDefender, che integra l'ultima soluzione di sicurezza di BitDefender per Linux nel CD GNU/Linux Knoppix Live, offrendo un antivirus di desktop capace di eseguire la scansione e disinfettare tutti i dischi rigidi esistenti (includendo partizioni NTFS di Windows). Nello stesso tempo BitDefender Rescue CD può essere utilizzato per ripristinare i vostri dati preziosi quando non si può avviare Windows

Nota

Il BitDefender Rescue CD può essere scaricato da: http://download.bitdefender.com/rescue_cd/

41.1. Requisiti del sistema

Prima di avviare BitDefender Rescue CD, dovete innanzitutto verificare se il vostro sistema ha i seguenti requisiti.

Tipo di processore

Compatibile x86, minimo 166 MHz, ma non sperare un alto rendimento in questo caso. Un processore di generazione i686, a 800 MHz sarebbe una scelta migliore.

Memoria

Minimo 512 MB di Memoria RAM (raccomandati 1 GB)

CD-ROM

BitDefender Rescue CD si esegue da un CD-ROM, per cui sono richiesti un CD-ROM ed un BIOS in grado di avviarlo.

Connessione Internet

Anche se BitDefender Rescue CD funzionerà senza connessione alla rete, le procedure di aggiornamento richiederanno un link HTTP attivo, persino attraverso alcuni server proxy. Di conseguenza, per una protezione aggiornata, la connessione ad Internet è obbligatoria.

Risoluzione grafica

Scheda grafica standard SVGA-compatibile.

41.2. Software Incluso

Il CD di soccorso BitDefender include i seguenti pacchetti software.

Xedit
Questo è un editore di file di testo.

Vim
Questo è un potente editore di file di testo, contenente evidenziatore di sintassi, un GUI, e molto altro.Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Vim.

Xcalc
Questa è una calcolatrice.

RoxFiler
RoxFiler è un veloce e potente gestore di file grafici.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di RoxFiler.

MidnightCommander
GNU Midnight Commander (mc) è un gestore di file text-mode.

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di MC .

Pstree
Pstree mostra i processi in corso.

Top
Top mostra le funzioni Linux.

Xkill
Xkill blocca tutte le X risorse di un client.

Partition Image
Partition Image vi aiuta a salvare le partizioni nei formati dei file di sistema EXT2, Reiserfs, NTFS, HPFS, FAT16, e FAT32 in un file di immagine. Questo programma può essere utile a fini di backup.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Partimage.

GtkRecover
GtkRecover è una versione GTK del console del programma di recupero. Aiuta a recuperare dei file.

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di GtkRecover.

ChkRootKit
ChkRootKit è uno strumento che vi aiuta ad effettuare la scansione del vostro computer in cerca di rootkits.

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di ChkRootKit.

Nessus Network Scanner
Nessus è uno scanner di sicurezza remota per Linux, Solaris, FreeBSD, e Mac OS X.

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di Nessus.

Iptraf
Iptraf è un Software di monitoraggio di rete IP.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Iptraf.

Iftop
Iftop mostra l'uso di larghezza di banda su di un interfaccia.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Iftop.

MTR
MTR è uno strumento di diagnosi di rete.

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di MTR .

PPPStatus
PPPStatus mostra le statistiche sul traffico TCP/IP in entrata ed in uscita.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di PPPStatus.

Wavemon
Wavemon è un'applicazione di monitoraggio per dispositivi di rete wireless.

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di Wavemon.

USBView
USBView mostra informazioni sui dispositivi connessi al bus USB.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di USBView.

Pppconfig
Pppconfig aiuta a configurare automaticamente una connessione dial up ppp.

DSL/PPPoe
DSL/PPPoe configura una connessione PPPoE (ADSL).

I810rotate
I810rotate cambia l'output su video a i810 hardware usando i810switch(1).

Per ulteriori informazioni, vi preghiamo di riferirvi allahomepage di I810rotate .

Mutt
Mutt è un potente mail client MIME basato su testo.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Mutt.

Mozilla Firefox
Mozilla Firefox è un noto browser web.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Mozilla Firefox.

Elinks

Elinks browser di web in modo testo.

Per ulteriori informazioni, vi preghiamo di riferirvi alla homepage di Elinks.

42. BitDefender Rescue CD fai-da-te.

Questo capitolo contiene informazioni su come iniziare e fermare il BitDefender Rescue CD, come eseguire la scansione del vostro computer alla ricerca di malware e anche come salvare dati dal vostro PC Windows compromesso su un dispositivo rimuovibile. In ogni caso, utilizzando le applicazioni software contenute nel CD, potrete eseguire molti processi, la cui descrizione va oltre gli obiettivi di questo manuale.

42.1. Avviare BitDefender Rescue CD

Per avviare il CD, configura il BIOS del tuo computer per avviarsi dal CD, inserisci il CD nell'unità e riavvia il computer. Assicurati che il tuo computer possa avviarsi dal CD.

Attendere che venga mostrata la finestra successiva e seguire le istruzioni per avviare BitDefender Rescue CD.

Boot Splash Screen

Al avvio, l'aggiornamento delle impronte dei virus viene eseguito automaticamente. Questo potrebbe richiedere qualche istante.

Quando il processo di avvio è finito si vedrà poi il desktop. Adesso è possibile cominciare ad utilizzare il BitDefender Rescue CD.

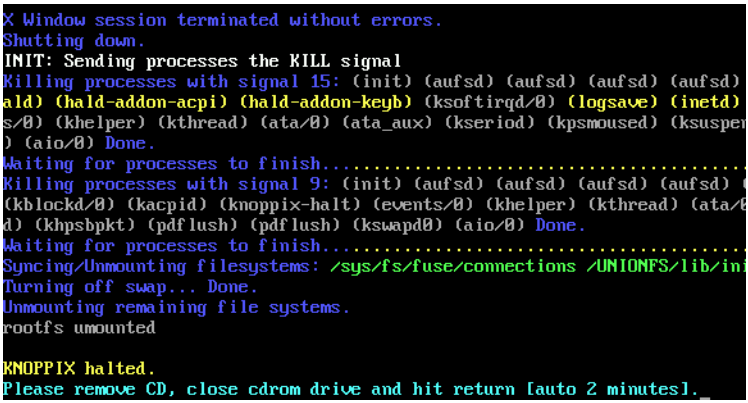
Il Desktop

42.2. Arrestare BitDefender Rescue CD

È possibile spegnere il computer in modo sicuro selezionando **Uscire** dal menu contestuale di BitDefender Rescue CD (fare clic con il pulsante destro per aprirlo) o usando il comando **Ferma** su un terminale.

Scegli “Uscire”

Quando BitDefender Rescue CD avrà chiuso tutti i programmi con successo, mostrerà una schermata come l’immagine seguente. Potrete rimuovere il CD per fare l'avvio dall' hard disk. Adesso potete spegnere oppure riavviare il vostro computer.


X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufsd) (aufsd) (aufsd) (aufsd)
ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksuspe
) (aio/0) Done.
Waiting for processes to finish.....
Killing processes with signal 9: (init) (aufsd) (aufsd) (aufsd) (aufsd)
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/
d) (khpsbpkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.....
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/in
Turning off swap... Done.
Unmounting remaining file systems.
rootfs umounted
KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes].

Attendi questo messaggio alla chiusura

42.3. Come eseguo una scansione antivirus?

Apparirà una procedura guidata quando il processo di avvio sarà terminato che permetterà di eseguire una scansione completa del computer. È sufficiente fare clic sul pulsante **Avvia**.

Nota
Se la risoluzione del vostro schermo non è abbastanza alta, vi verrà chiesto di cominciare la scansione in modalità di testo.

Seguire la procedura di tre passi per completare il processo di scansione.

1. Potete visualizzare lo stato della scansione e le statistiche (velocità di scansione, tempo trascorso, numero di oggetti esaminati / infetti / sospetti / nascosti ed altro).

   Nota
   La durata del processo dipende dalla complessità della scansione.

2. Si potrà vedere il numero di problemi che colpiscono il vs. sistema.

   I problemi vengono mostrati in gruppi. Selezionare la casella "+" per aprire un gruppo oppure la casella "-" per chiudere un gruppo.

   Potete scegliere di intraprendere un'azione globale per ogni gruppo di problemi oppure selezionare azioni separate per ogni problema.
3. E' possibile visualizzare il sommario dei risultati.

Se si desidera scansionare solo una certa directory, è possibile utilizzare una delle seguenti alternative:

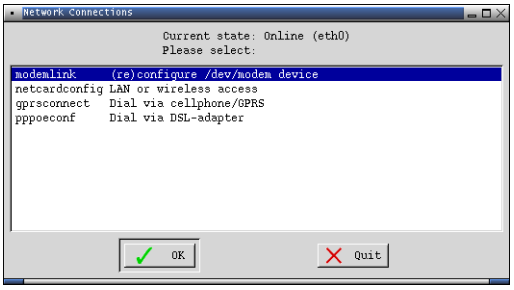
- Utilizzare **Scanner BitDefender per Unix**.
  1. Fare un doppio clic sull'icona AVVIA SCANNER sul Desktop. Verrà avviato lo **Scanner BitDefender per Unix**.
  2. Fare clic su **Scanner**, apparirà una nuova finestra.
  3. Selezionare la directory che si desidera scansionare e fare clic su **Apri** per avviare la scansione utilizzando la stessa procedura guidata quando si avviato il computer la prima volta.
- Usare il menu contestuale - cercare le cartelle, fare clic con il pulsante destro su un file o una directory e selezionare **Invia a**. Quindi scegliere **Scanner BitDefender**.
- O puoi emettere questo commando come ruta, da un terminale. Lo **BitDefender Antivirus Scanner** commincierà con il file o cartella selezionato come ubicazione predefinita da eseguire la scansione.

```
# bdscan /path/to/scan/
```

42.4. Come Configurare la connessione Internet?

Se sei in una rete DHCP ed hai una scheda di rete ethernet, la connessione Internet dovrebbe già essere rilevata e configurata. Per una configurazione manuale, segue questi passi.

1. Cliccare due volte sull'icona Risorse di Rete sul Desktop. Apparirà la seguente finestra.



Connessioni di rete

2. Selezionare il tipo di connessione che state usando e cliccare su OK.

Connessione	Descrizione
modemlink	Selezionare questo tipo di connessione se state usando un modem ed una linea telefonica per accedere ad Internet.
netcardconfig	Selezionare questo tipo di connessione se state usando connessione alla rete locale (LAN) per accedere ad Internet. E' anche adeguato per le connessioni wireless.
gprsconnect	Selezionare questo tipo di connessione se accedete ad Internet tramite rete cellulare usando il protocollo GPRS (General Packet Radio Service). Ovviamente potete anche usare un modem GPRS al posto del cellulare.
pppoeconf	Selezionare questo tipo di connessione se usate un modem DSL (Digital Subscriber Line) per accedere ad Internet.

3. Seguire le istruzioni sullo schermo. Se non siete sicuri di cosa scrivere, contattate il vostro amministratore di sistema o della rete per i dettagli.

Importante

Tenere presente che selezionando una delle opzioni citate sopra attivate solo il modem. Per configurare la connessione di rete, seguire questi passi.

1. Fare clic con il pulsante destro sul desktop. Apparirà il menu contestuale del BitDefender Rescue CD.
2. Selezionare **Terminale (come radice)**.
3. Digitare i seguenti comandi:

```
# pppconfig
```

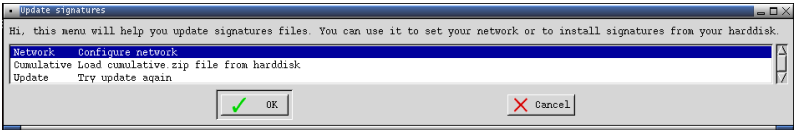
4. Seguire le istruzioni sullo schermo. Se non siete sicuri di cosa scrivere, contattate il vostro amministratore di sistema o della rete per i dettagli.

42.5. Come aggiornare BitDefender?

Al momento dell'avvio, l'aggiornamento delle firme virus viene fatto automaticamente. Tuttavia, se si salta questo passo o si desidera semplicemente eseguire un aggiornamento dopo l'avvio, ecco due modi aggiornare BitDefender.

- Utilizzare **Scanner BitDefender per Unix**.
  1. Fare un doppio clic sull'icona AVVIA SCANNER sul desktop. Verrà avviato lo **Scanner BitDefender per Unix**.
  2. Fare clic su **Aggiorna**.
- Utilizzare il collegamento **Aggiorna firme** sul desktop.

1. Cliccare due volte sul collegamento sul Desktop Aggiornare Impronte. Apparirà la seguente finestra.


Update signatures
Hi, this menu will help you update signatures files. You can use it to set your network or to install signatures from your harddisk.
Network Configure network
Cumulative Load cumulative zip file from harddisk
Update Try update again
OK
Cancel

Aggiornare impronte.

2. Eseguire una delle seguenti azioni:
   - Selezionare **Cumulativo** per installare le impronte già salvate sul vostro disco rigido sfogliando il computer e caricando il file `cumulativo.zip`.
   - Selezionare **Aggiornare** per connettersi immediatamente ad Internet e scaricare le impronte di virus più recenti.
3. Selezionare **OK**.

42.5.1. Come aggiornare BitDefender attraverso un proxy?

Se ci fosse un server proxy tra il computer ed Internet, è necessario impostare alcune configurazioni per poter aggiornare le firme dei virus.

Per aggiornare BitDefender su un proxy, utilizzare una delle seguenti opzioni:

- Utilizzare **Scanner BitDefender per Unix**.
  1. Fare un doppio clic sull'icona AVVIA SCANNER sul Desktop. Verrà avviato lo **Scanner BitDefender per Unix**.
  2. Fare clic su **Impostazioni**, apparirà una nuova finestra.
  3. In **Aggiorna impostazioni**, selezionare la casella di controllo **Abilita Proxy HTTP**. Specificare l'host Proxy (nel seguente formato: `host[:port]`), l'utente proxy (nel seguente formato: `[domain\]username`) e la password. Selezionare la casella di controllo **Scavalca server proxy quando non è disponibile** per una connessione diretta da utilizzare quando il server proxy non è disponibile.
  4. Fare clic su **Salva**
  5. Fare clic su **Aggiorna**
- Usa terminale (come radice).
  1. Fare clic con il pulsante destro sul desktop. Apparirà il menu contestuale del BitDefender Rescue CD.
  2. Selezionare **Terminale (come radice)**.
  3. Digitare il comando: **cd /ramdisk/BitDefender-scanner/etc**.
  4. Digitare il comando: **mcedit bdscan.conf** per modificare questo file usando GNU Midnight Commander (mc).

5. Cancellare la seguente linea: `#HttpProxy =` (eliminare solo il segno #) e specificare il dominio, nome utente, password e porta del serve proxy. Ad esempio, la linea corrispondente dovrebbe essere così:

   ```
   HttpProxy = myuser:mypassword@proxy.company.com:8080
   ```
6. Premere **F2** per salvare il file corrente, confermare il salvataggio e quindi premere **F10** per chiuderlo.
7. Digitare il comando: **bdscan update**.

42.6. Come posso salvare ai miei dati?

Supponiamo che non potete avviare il vostro PC Windows a causa di problemi sconosciuti. Nello stesso tempo, avete un bisogno disperato di accedere ad alcuni dati importanti sul vostro computer. Questo è il momento in cui BitDefender Rescue CD diventa utile.

Per salvare i vostri dati dal computer ad un dispositivo rimuovibile, come una penna USB, basta seguire questi passaggi:

1. Inserire BitDefender Rescue CD nel lettore CD, la penna USB nella porta USB e quindi riavviare il computer.

   Nota

   Se inserite la penna USB in un secondo momento, dovrete montare il disco rimovibile seguendo questi passaggi:

   a. Cliccare due volte sul collegamento sul Desktop Terminal Emulator.

   b. Digitare il seguente comando:

   ```
   # mount  /media/sdb1
   ```

   Tenere presente che a seconda della configuarzione del vostro computer esso potrà essere `sda1` invece di `sdb1`.

2. Attendere finchè BitDefender Rescue CD completi l'avvio. Apparirà la seguente finestra.

Schermo del Desktop

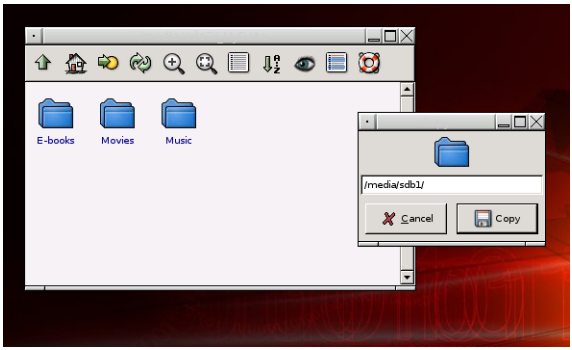
3. Cliccare due volte sulla partizione dove sono ubicati i dati che volete salvare (e.g. `[sda3]`).

   Nota
   Quando lavorate con BitDefender Rescue CD, avrete a che fare con nomi di partizioni Linux. Quindi, `[sda1]` probabilmente corrisponderà alla partizione Windows `(C:)`, `[sda3]` alla `(F:)`, e `[sdb1]` alla penna USB.

   Importante
   Se il computer non è stato spento correttamente è possibile che alcune partizioni non siano state montate automaticamente. Per montare una partizione, seguire questi passi.
   a. Cliccare due volte sul collegamento sul Desktop Terminal Emulator.
   b. Digitare il seguente comando:

   ```
   # mount  /media/partition_name
   ```

4. Sfogliare le vostre cartelle ed aprire la directory desiderata. Per esempio, `MyData`, contenente le sottodirectory`Movies`, `Music` ed `E-books`.
5. Fare clic con il pulsante destro sulla directory desiderata e selezionare **Copia**. Apparirà la seguente finestra.



Salvataggio dei dati

6. Scrivere `/media/sdb1/` nella corrispondente casella di testo e cliccare **Copiare**.

   Tenere presente che a seconda della configuarzione del vostro computer esso potrà essere `sda1` invece di `sdb1`.

42.7. Come si usa la modalità console?

Se la risoluzione dello schermo non è abbastanza alta per avviare l'interfaccia utente grafica, è possibile eseguire il CD di recupero BitDefender nella modalità console. La modalità testo semplice consente di eseguire una scansione completa del proprio.

Per eseguire il CD nella modalità console, impostare il BIOS del computer per avviarsi dal CD, mettere il CD nel drive e riavviare il computer. Attendere lo schermo di caricamento e selezionare **Avvia knoppix nella modalità console**.

Dopo l'avvio, seguire le istruzioni sullo schermo per eseguire una scansione completa del computer.

BitDefender rileva le partizioni sul proprio disco rigido e aggiorna automaticamente il database delle firme malware prima dell'inizio della scansione. Se vengono trovati dei file infetti, BitDefender li disinfetterà. Dopo il completamento del processo di scansione, viene visualizzato il registro di scansione.

Nota
La durata del processo dipende dalla complessità della scansione.

Glossario

ActiveX

ActiveX è una modalità di scrittura dei Programmi affinché possano essere invocati da altri Programmi e sistemi operativi. La tecnologia ActiveX viene utilizzata con Microsoft Internet Explorer per generare pagine Web interattive che sembrino e si comportino come applicazioni e non come semplici pagine statiche. Con gli elementi ActiveX, gli utenti possono chiedere o rispondere a domande, adoperare dei pulsanti ed interagire in altri modi con la pagina Web. I controlli ActiveX vengono spesso scritti utilizzando il linguaggio Visual Basic.

Gli ActiveX sono noti per una totale mancanza di controlli di sicurezza; gli esperti di sicurezza dei computer scoraggiano il loro utilizzo attraverso Internet.

Adware

L' adware è spesso combinato con un' applicazione Host offerta senza spese quando l'utente accetta l'adware. Le applicazioni adware vengono di solito installate dopo che l'utente ha accettato l'accordo di licenza, dove si spiega il proposito della applicazione. Non viene commesa quindi alcuna offesa o scortesia.

Comunque, i pop-up di avvertimento possono rappresentare un fastidio, ed in alcuni casi degrada il funzionamento del sistema. Inoltre, l'informazione che viene raccolta da queste applicazioni può causare inconvenienti riguardo alla privacy degli utenti non completamente ben informati sui termini del'accordo di licenza.

Archivia

Disco, nastro o cartella che contiene file memorizzati.

Un file che contiene uno o più file in forma compressa.

Backdoor

Breccia nella sicurezza di un programma deliberatamente implementata dal costruttore o dal manutentore. La presenza di tali "brecce" non sempre è dolosa: su alcuni sistemi operativi, ad esempio, vengono utilizzate per l'accesso con utenze privilegiate per servizi tecnici o per i programmatori del venditore a scopo di manutenzione.

Settore di boot

Settore all'inizio di ogni disco che identifica l'architettura del disco (dimensione del settore, dimensione del cluster, ecc.). Nei dischi di avvio, il settore di boot contiene anche un programma che carica il sistema operativo.

Virus di boot

Virus che infetta il settore di boot di un disco rigido oppure di un'unità floppy. Qualsiasi tentativo di effettuare il boot da un disco floppy infetto con un virus di boot, farà sì che il virus venga attivato nella memoria. Da quel momento in

poi, ogni volta che si esegue il boot del sistema, il virus sarà attivo nella memoria.

Browser

Abbreviazione di Web browser, un'applicazione software utilizzata per localizzare e visualizzare pagine Web. I due browser più noti sono Netscape Navigator e Microsoft Internet Explorer. Entrambi sono Browser grafici, ovvero in grado di visualizzare sia grafici che testo. Inoltre, i browser più moderni possono presentare informazioni multimediali, incluso suoni e animazione, nonostante richiedano i plug-in per alcuni formati.

Linea di commando

In un'interfaccia a linea di comando, l'utente digita i comandi nello spazio previsto direttamente sullo schermo, utilizzando il linguaggio di commando.

Cookies

Nell'industria di Internet, i cookie vengono descritti come piccoli file contenenti informazioni relative ai computer individuali che possono essere analizzate e utilizzate dai pubblicitari per tenere traccia dei vostri interessi e gusti online. In questo regno, la tecnologia dei cookie è ancora in fase di sviluppo e l'intenzione è quella di fornire direttamente ciò che si dichiara essere il proprio interesse. Per molte persone è una lama a doppio taglio, poiché da una parte è efficace e consente di far vedere solo ciò che viene dichiarato interessante. Dall'altra parte, implica in effetti un "tracciamento" di dove si va e di cosa si seleziona. Comprensibilmente in questo modo nascerà un dibattito relativo alla riservatezza e molte persone si sentono offese all'idea di essere visti come un " SKU number" (il codice a barre sul retro delle confezioni che vengono passati alla scansione della cassa). Se questo punto di vista può essere considerato estremo, in alcuni casi può essere corretto.

Disk drive

È un dispositivo che legge e scrive dei dati su un disco.

Un drive di disco rigido legge e scrive dischi rigidi.

Un drive di floppy accede i dischi floppy.

I drive di disco possono essere interni (incorporati all'interno di un computer) oppure esterni (collocati in un meccanismo separato e connesso al computer).

Download

Per copiare dati (solitamente un file intero) da un'origine principale su un dispositivo periferico. Il termine viene spesso utilizzato per descrivere un processo di copia di un documento da un servizio on-line sul computer di un utente. Si può inoltre riferire al processo di copiatura di un file da un file server di rete su un computer della rete.

E-mail

Posta elettronica. Servizio che invia messaggi ai computer attraverso reti locali o globali.

Eventi

Azione oppure avvenimento rilevato da un programma. Gli eventi possono rappresentare azioni dell'utente, come fare un clic con il mouse o premere un tasto sulla tastiera oppure avvenimenti del sistema, ad esempio memoria insufficiente.

Falso positivo

Appare quando un prodotto di analisi antivirus individua un documento come infettato quando di fatto non lo è.

Estensione del nome di un file

Porzione del nome di un file che segue il punto finale e che indica il tipo di dati inclusi nel file.

Molti sistemi operativi utilizzano estensioni del nome del file, come Unix, VMS e MS-DOS. Sono normalmente composti da uno a tre lettere (alcuni vecchi supporti OS non più di tre). Esempi: "c" per codici sorgente C, "ps" per PostScipt, "txt" per testi arbitrari.

Euristico

Un metodo basato su regole per l'identificazione di nuovi virus. Questo metodo di scansione non si basa su specifiche impronte dei virus. Il vantaggio della scansione euristica è di non venire ingannata dalle nuove varianti dei virus esistenti. Può comunque occasionalmente segnalare codici sospetti in programmi normali, generando "falsi positivi".

IP

Internet Protocol – protocollo di instradamento nella suite di protocollo TCP/IP, responsabile dell'indirizzamento IP, dell'instradamento, della frammentazione e della ricomposizione dei pacchetti IP.

Applet Java

Programma Java concepito per funzionare solo su pagine web. Per utilizzare un applet su una pagina web, bisognerà specificare il nome dell'applet e la dimensione (lunghezza e larghezza -in pixel) che l'applet può utilizzare. Quando si accede alla pagina web, il browser scarica l'applet dal server e lo esegue sulla macchina dell'utente (il client). Gli Applet differiscono dalle applicazioni in quanto sono governati da un rigido protocollo di sicurezza.

Ad esempio, nonostante gli applet vengano lanciati sul client, essi non possono leggere o scrivere dati nella macchina dell'utente. Inoltre, gli applet sono ulteriormente limitati in modo che possano leggere e scrivere dati solo dallo stesso dominio dai quali provengono.

Macro virus

Tipo di virus del computer codificato come macro all'interno di un documento. Molte applicazioni, come ad esempio Microsoft Word ed Excel, supportano potenti linguaggi macro.

Queste applicazioni consentono di codificare una macro in un documento e di eseguire la macro ogni volta che il documento viene aperto.

Client mail

Un client e-mail è un'applicazione che vi consente di inviare e ricevere e-mail.

Memoria

Aree di immagazzinaggio interne nel computer. Il termine memoria identifica l'immagazzinaggio dati sotto forma di chip; la parola storage viene utilizzata per la memoria su nastri o su dischi. Ogni computer dispone di un certo quantitativo di memoria fisica, solitamente chiamata memoria principale oppure RAM.

Non euristico

Questo metodo di scansione si basa su specifiche impronte di virus. Il vantaggio della scansione non-euristica è di non essere ingannato da ciò che potrebbe sembrare un virus e non genera falsi allarmi.

Programmi impaccati

File in formato compresso. Molti sistemi operativi e molte applicazioni contengono comandi che vi consentono di impaccare un file in modo da occupare meno memoria. Ad esempio, supponiamo che abbiate un file di testo che contenga dieci caratteri spazio consecutivi. Normalmente occuperebbe dieci byte di memoria.

Un programma che impacca i file sostituirebbe gli spazi con un carattere speciale serie_di_spazi seguito dal numero di spazi sostituiti. In questo caso i dieci spazi occuperebbero solo due byte. Questa è solo una tecnica di impaccaggio – ce ne sono molte altre.

Percorso

Le esatte direzioni per raggiungere un file su un computer. Queste direzioni vengono solitamente descritte attraverso il sistema di casellario gerarchico dall'alto al basso.

La strada tra due punti qualsiasi, come ad esempio il canale di comunicazioni tra due computer.

Phishing

L'atto d'inviare una mail ad un utente fingendo di essere una ditta legittima ed affermata, nel tentativo di truffare l'utente, facendole cedere informazione privata che verrà usata per furti d'identità. La e-mail indirizza gli utenti a visitare una pagina Web, dove gli viene chiesto di aggiornare informazioni personali, come password e carte di credito, numero della previdenza sociale e del conto

in banca, che questa legittima organizzazione ha già. In ogni caso, la pagina Web è finta, e organizzata soltanto per rubare l'informazione del utente.

Virus polimorfico

Virus che modifica la propria forma con ogni file che infetta. In quanto non dispongono di caratteristiche binarie costanti, tali virus sono difficili da identificare.

Porta

Interfaccia su un computer alla quale è possibile connettere un supporto. I Personal Computer hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, schermi e tastiere. Esternamente i Personal Computer hanno porte per la connessione dei modem, delle stampanti, dei mouse e altri supporti periferici.

Nelle reti TCP/IP e UDP, un punto di arrivo ad una connessione logica. Il numero della porta identifica di che tipo di porta si tratta. Ad esempio, la porta 80 viene usata per il traffico HTTP.

File di report

File che elenca le azioni avvenute. BitDefender mantiene un file di rapporto che elenca i percorsi esaminati, le cartelle, il numero di archivi e file esaminati, quanti file infetti e sospetti sono stati trovati.

Rootkit

Un rootkit è una serie di strumenti software che offre accesso a livello di amministratore ad un sistema. Il termine fu usato per la prima volta per i sistemi operativi UNIX e faceva riferimento a strumenti ricompilati che fornivano agli intrusi i diritti di amministratore, consentendo loro di celare la loro presenza in modo da non dover essere visti dagli amministratori del sistema.

Il ruolo principale dei rootkit è nascondere i processi, i file, i login e i log. Possono anche intercettare dati dai terminali, dalle connessioni di rete o dalle periferiche, se incorporano il software adeguato.

I rootkit non sono maligni per natura. Ad esempio, i sistemi e persino alcune applicazioni nascondono file critici utilizzando rootkit. Comunque, essi vengono principalmente utilizzati per nascondere malware o per celare la presenza di un intruso nel sistema. Se combinati al malware, i rootkit rappresentano una grave minaccia per l'integrità e la sicurezza di un sistema. Possono monitorare il traffico, creare backdoor nel sistema, alterare file e log ed evitare il rilevamento.

Script

Altro termine per macro o file batch, uno script è una lista di comandi che possono essere eseguiti senza interazione con l'utente.

Spam

Posta elettronica pubblicitaria. Generalmente conosciuto come qualsiasi e-mail non richiesta.

Spyware

Accede alla connessione internet dell'utente senza che l'utente se ne accorga, normalmente a scopo pubblicitario. Le applicazioni Spyware vengono tipicamente come un componente nascosto di programmi freeware o shareware che possono essere scaricati da Internet. Tuttavia, deve essere segnalato che la maggioranza delle applicazioni shareware o freeware non arrivano con spyware. Una volta installato, lo spyware esegue il monitoraggio dell'attività dell' utente su Internet e trasmette questa informazione di nascosto a qualcun altro. Lo spyware può anche raccogliere informazione su indirizzi mail e addirittura passwords e numeri di carta di credito.

Lo spyware è simile a un Cavallo di Troia che gli utenti installano senza volere quando installano qualcos'altro. Un modo comune di diventare una vittima dello spyware è scaricare certi file peer-to-peer scambiando prodotti che sono disponibili oggi.

A parte delle questioni dell'etica e la privacy, lo spyware approfitta dell' utente usando risorse di memoria del computer "mangiandosi" larghezza di banda dal momento in cui invia informazione alla sua "casa" usando l' internet dell' utente. Dato che lo spyware sta usando memoria e risorse del sistema, le applicazioni eseguite in sottofondo (background) possono portare alla caduta del sistema o alla instabilità.

Elementi di startup

Qualsiasi file posizionato in questa cartella si aprirà quando il computer viene avviato. Ad esempio, una schermata di avvio, un file sonoro da eseguire quando il computer si avvia la prima volta, una agenda-calendario, oppure programmi applicativi che possono essere elementi di startup. Normalmente in questa cartella viene posizionato un alias di un file, anziché il file stesso.

Barra di sistema

Introdotta con Windows 95, la barra delle applicazioni è situata nella barra degli strumenti di Windows (solitamente in basso vicino all'orologio) e contiene icone miniaturizzate per un semplice accesso alle funzioni di sistema, ad esempio il fax, la stampante, il modem, il volume ed altro. Fare doppio clic o fare clic con il pulsante destro su un'icona per vedere ed accedere ai dettagli e ai controlli.

TCP/IP

Transmission Control Protocol/Internet Protocol – Insieme di protocolli di networking largamente utilizzati su Internet che consentono le comunicazioni attraverso le reti interconnesse di computer con diverse architetture hardware e vari sistemi operativi. TCP/IP include gli standard su come comunicano i computer e le convenzioni per connettere le reti e il traffico di instradamento.

Trojan

Programma distruttivo che si maschera da applicazione benevola. Diversamente dai virus, i cavalli di Troia non si replicano ma possono comunque essere altrettanto distruttivi. Un tipo di cavallo di Troia particolarmente insidioso è un programma che dichiara di pulire i virus del vostro computer ma che al contrario introduce i virus nel vostro computer.

Il termine deriva dalla storia dell'Iliade di Omero, dove i Greci mandarono un gigantesco cavallo di legno ai loro avversari, i Troiani, apparentemente come offerta di pace. Ma dopo che i Troiani portarono il cavallo all'interno delle mura della loro città, i soldati Greci uscirono dal ventre cavo del cavallo e aprirono le porte della città, consentendo ai loro compatrioti di entrare e catturare Troia.

Aggiorna

La nuova versione di un prodotto software o hardware creato per sostituire una versione precedente dello stesso prodotto. In aggiunta, le routine di installazione degli aggiornamenti spesso verificano e si assicurano che sia già installata una versione precedente sul vostro computer; diversamente non sarà possibile installare l'aggiornamento.

BitDefender dispone del proprio modulo di aggiornamento che consente la verifica manuale degli aggiornamenti oppure l'aggiornamento automatico del prodotto.

Virus

Programma o parte di codice caricato sul vostro computer senza che voi lo sappiate e che viene eseguito contro la vostra volontà. La maggior parte dei virus è anche in grado di auto replicarsi. Tutti i virus del computer sono creati dall'uomo. E' relativamente facile produrre un semplice virus in grado di copiare sé stesso innumerevoli volte. Persino un virus così semplice è pericoloso in quanto utilizzerà velocemente tutta la memoria disponibile e porterà il sistema allo stallo. Un tipo di virus ancora più pericoloso è quello in grado di trasmettere sé stesso attraverso le reti superando i sistemi di sicurezza.

Definizione di virus

Caratteristica binaria di un virus, utilizzata dal programma antivirus alfine di rilevare ed eliminare il virus stesso.

Worm(baco)

Programma che si propaga in una rete, riproducendosi durante lo spostamento. Non si può attaccare ad altri programmi.